FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0 and 9

[PS Docket Nos. 21-479 and 13-75, FCC 26-39; FR ID 355738]

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

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (the FCC or Commission) adopts rules to ensure that emerging Next Generation 911 (NG911) networks are reliable and interoperable. NG911 is replacing legacy 911 technology across the country with Internet Protocol (IP)-based infrastructure that will support new 911 capabilities, including text, video, and data. However, for NG911 to be fully effective, NG911 networks must be designed to safeguard the reliability of critical components and support the interoperability needed to seamlessly transfer 911 calls and data from one network to another. The rules require entities essential to delivering emergency calls in the NG911 environment to implement common sense measures to safeguard the reliability of NG911 networks and reduce the risk of 911 outages, and require certain entities to report on their support for NG911 interoperability. The rules also eliminate unnecessary and burdensome legacy rules to increase flexibility and encourage technical innovation to make NG911 services reliable, interoperable, and accessible to all.

DATES: *Effective date*: Effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

Compliance dates: Compliance will not be required for §§ 9.19(c)(1)(i) through (c)(3)(i) and 9.20(a)(1)(i), (a)(2)(i), and (b), until a document is published in the *Federal Register* announcing compliance dates and revising §§ 9.20(a)(1)(i), (a)(2)(i), and (b), and revising or removing §§ 9.19(d) and 9.20(h). For entities described in § 9.19(a)(4)(i)(E) through (I), compliance with §

9.19(b) will not be required until a document is published in the *Federal Register* announcing compliance dates and revising or removing § 9.19(d).

FOR FURTHER INFORMATION CONTACT: Rachel Waxman, Deputy Division Chief, Policy and Licensing Division, Public Safety and Homeland Security Bureau, at (202) 418-1138 or Rachel.Waxman@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Second Report and Order (*Order*), in PS Docket Nos. 21-479 and 13-75, FCC 26-39, adopted on June 25, 2026, and released on June 26, 2026. The full text of this document is available at https://www.fcc.gov/document/fcc-modernizes-next-generation-911-reliability-and-interoperability-0.

People with Disabilities. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530.

Congressional Review Act. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this *Second Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

Synopsis

Introduction

Today, we modernize the Commission's 911 reliability framework to reflect America's ongoing upgrade to modern high-speed telecommunications infrastructure. 911 Authorities are rapidly replacing legacy 911 systems and migrating to the Next Generation 911 (NG911) ecosystem to gain access to advanced capabilities, enhanced resilience, greater interoperability,

and improved accessibility.[1] In this Second Report and Order (*Order)*, we ensure the reliability of NG911 by leveraging the strengths of modern telecommunications networks, including high-capacity fiber, dynamic routing, automated monitoring, and real-time failover capabilities that do not exist in legacy systems.

As the nation has embarked on the transition to NG911 over the last decade, the Commission has seen a corresponding increase in major, multi-state 911 service outages that have disrupted access to life-saving emergency services for millions of Americans.[2] Too often, these outages have occurred in parts of transitional NG911 systems outside the scope of the 911 reliability framework adopted in 2013,[3] which does not address the increasingly complex array of call scenarios in the Internet Protocol (IP) call origination context we live in today. We believe that, in many of these instances, operators could have prevented or mitigated outages by implementing reliability measures appropriate for IP-based systems.[4]

Because the 2013 911 reliability framework cannot reliably support modern 911 call flows, we take the following actions to reduce the risk of future outages in transitional and end-state NG911 networks and to streamline and reduce the burdens of our approach:

- *Covered 911 service providers*. We update our definition of covered 911 service providers (CSPs) to identify categories of providers whose operations are essential to NG911 call delivery, whose failure could cause significant outages, and who therefore must meet enhanced reliability standards under the Commission's framework. Our updated CSP definition includes operators of Emergency Services IP networks (ESInets), Next Generation Core Services (NGCS) providers, and providers of real-time location

[1] NG911 is an Internet Protocol (IP)-based system that enables emergency communications centers to receive, process, and analyze all types of 911 requests for emergency assistance; ensures interoperability; is secure; and meets certain other requirements. *See* 47 CFR § 9.28.
[2] *See, e.g.*, *Facilitating Implementation of Next Generation 911 Services (NG911)*, PS Docket Nos. 21-479 and 13-75, Further Notice of Proposed Rulemaking, 40 FCC Rcd 2668, 2676-77, para. 16 (2025) (*NG911 Reliability FNPRM*).
[3] *See Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket Nos. 13-75 and 11-60, Report and Order, 28 FCC Rcd 17476 (2013) (*911 Reliability Order*).
[4] *NG911 Reliability FNPRM* at 2677, para. 17.

services, major IP transport, IP 911 traffic aggregation, and essential gateways for converting legacy and IP traffic.

- *Reliability standards*. We modernize and streamline the 911 reliability benchmarks applicable to CSPs to reflect widely recognized best practices appropriate to IP-based 911 networks. These benchmarks incorporate well-established IP best practices in the areas of physical diversity, operational integrity, and network monitoring and reflect achievable standards identified by the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC).[5] We also make clear that CSPs can satisfy their reliability obligations by adopting reasonable alternative measures, including measures requested by state, territorial, local, or tribal 911 Authorities.[6]
- *Interoperability*. To support the seamless transfer of 911 calls and associated data across the NG911 ecosystem, we require NGCS and ESInet CSPs to report their recent actions to enable interstate NG911 interoperability, while seeking further comment on more detailed interoperability requirements. We also adopt a definition of "interoperability" specific to NG911 to provide clarity for both CSPs and 911 Authorities as NG911 deployments progress.
- *Certification Process*. We eliminate the requirement that CSPs file annual compliance certifications and adopt a streamlined filing process for CSPs going forward. We provide for an 18-month transition period, after which CSPs will file initial reliability certifications in conformance with the new rules, which they will need to update only in the event of material changes. This will reduce unnecessary regulatory burdens on CSPs

[5] CSRIC is a federal advisory committee that provides recommendations to the Commission on ways it can help ensure the security, reliability, and interoperability of communications systems. FCC, *Communications Security, Reliability, and Interoperability Council*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited May 19, 2026).

[6] A 911 Authority is a "State, territorial, regional, Tribal, or local governmental entity that operates or has administrative authority over all or any aspect of a communications network for the receipt of 911 traffic at NG911 Delivery Points and for the transmission of such traffic from that point to PSAPs." 47 CFR § 9.28. 911 Traffic is "[t]ransmissions consisting of all 911 calls . . . and/or 911 text messages," as well as location information, callback numbers, and routing information sent with the call and/or text message. 47 CFR § 9.28.

while focusing the certification process on essential information relevant to ensuring NG911 reliability.

- *Oversight*. We allow 911 Authorities to access CSP certifications and reports subject to confidentiality safeguards, and we codify the process of the Public Safety and Homeland Security Bureau (PSHSB or the Bureau) for investigating and remediating noncompliance, providing transparency to service providers.[7]

Background

The FCC's 911 Reliability Framework

The Commission first required CSPs to improve the reliability and resiliency of 911 communications networks following an unanticipated and severe derecho storm in 2012. The storm struck the Midwest and Mid-Atlantic regions of the United States, leaving millions of Americans without 911 service for up to several days.[8] The Bureau conducted a comprehensive inquiry and found that the impacts to 911 service largely could have been mitigated or avoided had more providers adopted then-current industry best practices for network reliability to protect their facilities.[9]

1. In 2013, the Commission adopted rules requiring CSPs to implement these best practices and other sound engineering principles on their networks in order to prevent future 911 outages.[10] At that time, most CSPs provided 911 functions and connectivity on the networks of Incumbent Local Exchange Carriers (ILECs) between legacy selective routers or location

---

[7] When outages do occur or are potentially imminent, the Commission imposes a distinct set of reporting, notification, and response requirements on various classes of service providers. *See*, *e.g.*, 47 CFR §§ 4.9(a)-(g), 4.11 (requiring cable, satellite, wireless, wireline, interconnected Voice over Internet Protocol (VoIP), and other providers to submit reports to the Commission if they experience significant outages on their networks), 4.9(h) (requiring these providers and CSPs to notify PSAPs that may be affected by significant outages), 4.17-4.18 (requiring certain providers to cooperate during disaster declarations and to submit status reports to the Commission). Nothing in this *Order* modifies those part 4 rules; this *Order* strictly addresses the CSP reliability requirements in part 9 of the Commission's rules.

[8] FCC Public Safety and Homeland Security Bureau, Impact of the June 2012 Derecho on Communications Networks and Services: Report and Recommendations at 1 (2013) (*Derecho Report*), http://www.fcc.gov/document/derecho-report-and-recommendations. The effects were particularly severe in northern Virginia, where four PSAPs in the densely-populated National Capital Region lost service completely, and in West Virginia, where eleven PSAPs could not receive 911 calls for as long as twelve hours. *Id.* at 28-34.

[9] *Id.* at 1-2.

[10] *See 911 Reliability Order*.

databases and PSAPs.[11] The Commission defined CSPs to include entities that operate central offices directly serving PSAPs, as well as providers of 911, Enhanced 911 (E911), or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities.[12] While recognizing the emergence of NG911, the Commission was not persuaded at that time "that NG911 technologies ha[d] evolved to the point that reliability certification rules should apply to entities beyond those that offer core services functionally equivalent to [legacy] 911 and E911 capabilities."[13]

The Commission required CSPs to annually certify their efforts to provide reliable 911 service with respect to circuit diversity, central-office backup power, and diverse network monitoring.[14] Specifically, CSPs must make efforts to achieve the following goals:

- *Circuit diversity*: Eliminating all single points of failure in critical 911 circuits; tagging those circuits; and conducting diversity audits annually.[15]
- *Central-office backup power*: Provisioning central offices that serve PSAPs directly or that host selective routers with sufficient backup power to sustain full functionality in the event of power outages and testing and maintaining all backup power equipment.[16]
- *Network Monitoring*: Implementing physically diverse network monitoring links and aggregation points where monitoring data are collected and conducting diversity audits of monitoring links and aggregation points annually.[17]

The Commission delegated oversight of the reliability rules and certification process to PSHSB. The Bureau established the 911 Reliability Certification System (911RCS) to receive

---

[11] *911 Reliability Order*, 28 FCC Rcd at 17489, para. 37. A public safety answering point (PSAP) is "[a]n answering point that has been designated to receive 911 calls and route them to emergency services personnel." 47 CFR § 9.3.
[12] *911 Reliability Order*, 28 FCC Rcd at 17488-89, para. 36.
[13] *Id.* at 17491, para. 42.
[14] *Id.* at 17503-26, paras. 80-138.
[15] 47 CFR § 9.19(c)(1).
[16] *Id.* § 9.19(c)(2).
[17] *Id.* § 9.19(c)(3).

filings and certifications, and it was empowered to review certifications, revise certification forms and procedures, investigate noncompliance, and order remedial action.[18]

Since adopting the reliability rules in 2013, the Commission has consistently observed that the rules would need to be updated to keep pace with the NG911 transition. For example, in a 2014 Policy Statement and Notice of Proposed Rulemaking on improving 911 governance, the Commission noted that it might need to update the rules to address changes in 911 technologies and the persistence of "sunny day" 911 outages.[19] And in 2015, the Commission reiterated its intent to consider "whether [the rules] should be revised or expanded to cover new best practices or additional entities that provide NG911 capabilities, or in light of our understanding about how NG911 networks may differ from legacy 911 service."[20]

In July 2024, the Commission adopted a national NG911 transition framework that has accelerated the growth of the NG911 ecosystem.[21] The new transition framework specifies a two-phased approach to guide the transition to NG911, in which 911 Authorities initiate each phase by submitting a valid request to originating service providers (OSPs) within the relevant jurisdiction, and OSPs must comply with NG911 requirements for that phase within a defined period.[22] In the *NG911 Transition Order*, the Commission defined "Next Generation 911" to

---

[18] *Id.* § 0.392(j).
[19] *911 Governance and Accountability, Improving 911 Reliability*, Policy Statement and Notice of Proposed Rulemaking, PS Docket Nos. 14-193 and 13-75, 29 FCC Rcd 14208, 14222, para. 32 (2014) (*2014 911 Reliability NPRM*).
[20] *Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket Nos. 13-75 and 11-60, Order on Reconsideration, 30 FCC Rcd 8650, 8655, para. 11 (2015) (*2015 911 Reliability Recon. Order*) (explaining further that providing CSPs with the flexibility to implement alternative measures was "essential to support and encourage the transition to NG911," because the 2013 rules do not afford another option for most NG911 CSPs to demonstrate their reliability). *See also* 47 CFR § 9.19(c)(1)(ii), 9.19(c)(2)(ii), 9.19(c)(3)(ii) (If necessary, a CSP may certify that one or more of the reliability requirements does not apply to its network and provide a supporting explanation.).
[21] *See generally Next Generation 911 (NG911) Valid Requests*, PS Docket No. 25-143.
[22] *Facilitating Implementation of Next Generation 911 Services (NG911)*, PS Docket No. 21-479, PS Docket No. 18-64, Report and Order, 39 FCC Rcd 8137, 8139, para. 3 (2024) (*NG911 Transition Order*). "Originating service providers" are defined for purposes of the NG911 transition rules as "[p]roviders that originate 911 traffic, specifically wireline providers; commercial mobile radio service (CMRS) providers, excluding mobile satellite service (MSS) operators to the same extent as set forth in § 9.10(a); covered text providers, as defined in § 9.10(q)(1); interconnected Voice over Internet Protocol (VoIP) providers, including all entities subject to subpart D of this part; and internet-based Telecommunications Relay Service (TRS) providers that are directly involved with routing 911 traffic, pursuant to subpart E of [part 9]." 47 CFR § 9.28.

include interoperability, security, use of commonly accepted standards, and other criteria.[23] It also noted the potential for NG911 to support improved reliability and interoperability and that some commenters had urged it to consider specific reliability and interoperability requirements.[24] The Commission deferred consideration of reliability, interoperability, and accessibility[25] proposals because at the time they were beyond the scope of the proceeding. The NG911 transition framework rules took effect in March 2025,[26] and since then, 911 Authorities have issued more than 190 requests to begin Phase 1 service and one request for Phase 2 service. The requests cover parts or all of twenty-eight states and encompass more than 2,200 PSAPs.[27]

2025 NG911 Reliability FNPRM. In March 2025, the Commission proposed to modernize the 911 reliability framework to better ensure the resiliency, reliability, interoperability, and accessibility of NG911 networks.[28] In particular, the Commission proposed to expand the definition of covered 911 service providers so that IP-based providers and facilities that have emerged as essential to NG911 are subject to FCC reliability standards. The Commission proposed to clarify that it had already defined certain NG911 core services as CSPs under the 2013 reliability rules, because they provide NG911 capabilities that are functionally equivalent to the call routing, automatic location information, and automatic number identification functions of covered legacy facilities.[29]

The Commission proposed to update the three 911 reliability benchmarks (physical diversity, network monitoring, and backup power) that identify presumptively-reasonable measures to reflect sound, industry-standard network practices that support the reliability of modern NG911 networks.[30] The proposed updated physical diversity benchmark included

---

[23] 47 CFR § 9.28.
[24] *NG911 Transition Order*, 39 FCC Rcd at 8220-28, paras. 182-197.
[25] *Id.* at 8217, 8218-19, paras. 174, 176, 179.
[26] *Public Safety and Homeland Security Bureau Announces Compliance Date and Provides Guidance on Information Collection for the Implementation of Next Generation 911*, Public Notice, 40 FCC Rcd 2057 (PSHSB 2025).
[27] *See* PS Docket No. 25-143.
[28] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2669, para. 1.
[29] *Id.* at 2680, para. 29.
[30] *Id.* at 2691-96, paras. 59-70.

ensuring automatic rerouting capabilities, load balancing, and the geographic distribution of routing facilities, transport nodes, and node links sufficient to eliminate all single points of failure.[31] The network monitoring proposal included monitoring critical NG911 facilities using geographically distributed automatic disruption detection and alarm mechanisms appropriate for IP systems.[32] The Commission proposed to update the backup power benchmark by renaming it "operational integrity" and defining it to include providing location information server (LIS) and legacy network gateway (LNG) facilities with continuous power to maintain operations and the capability to automatically switch over to geographically diverse facilities.[33] The Commission also proposed in the *NG911 Reliability FNPRM* a new requirement for ESInets to be interoperable.[34] Finally, the Commission proposed several reforms to its oversight of the CSP reliability certification process.[35]

Evolution of 911 Architecture

Like telecommunications networks generally, 911 networks are evolving from Time-Division Multiplex (TDM)-based architectures to IP-based architectures. As 911 Authorities transition to the NG911 ecosystem, they must entirely replace the circuit-switched architecture of legacy 911 with IP-based technologies and applications that provide all of the same functions as the legacy 911 system, as well as new capabilities. In its end state, NG911 will facilitate interoperability and system resilience, improve connections between PSAPs, and support the transmission of text, photos, videos, and data to PSAPs by individuals seeking emergency assistance. Many 911 Authorities have made significant progress to implement the transition to NG911.[36] As 911 architectures evolve, the entities that support essential functions and control

---

[31] *Id.* at 2693-95, paras. 62-66.
[32] *Id.* at 2695-96, paras. 67-68.
[33] *Id.* at 2696, paras. 69-70.
[34] An ESInet is an "(IP)-based network that is managed or operated by a 911 Authority or its agents or vendors and that is used for emergency services communications, including Next Generation 911." 47 CFR § 9.28.
[35] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2702-10, paras. 88-110.
[36] Forty-two states, the District of Columbia, Guam, and Puerto Rico reported expenditures on NG911 programs in calendar year 2024. FCC, Seventeenth Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges at 3 (2026), https://www.fcc.gov/sites/default/files/17thAnnual911FeeReport-021326.pdf. The total amount of reported NG911 expenditures in 2024 was $535,126,846.47. *Id.*

critical components and pathways on 911 networks also change. In considering the CSPs that must take reasonable measures to provide reliable 911 service, the Commission has monitored the changing roles and responsibilities of different entities within legacy, transitional, and NG911 network architectures.

Legacy 911 Networks

In 2013, when the Commission adopted the *911 Reliability Order*, the legacy networks of incumbent wireline providers typically connected PSAPs to those seeking help, whether the call for assistance originated on a landline or a wireless phone.[37] In these call flows, OSPs originate and transmit 911 calls placed by their customers, together with information about the callers' locations, to legacy 911 networks, where the calls are collected at an aggregation point called a selective router.[38] The selective router identifies the appropriate PSAP to receive each call by accessing an internal routing table that compares the caller's location information to the service areas of local PSAPs. The routing table data are populated with the assistance of a Master Street Address Guide (MSAG), a database that stores all valid physical addresses within each PSAP's service area, and an ANI/ALI database that pairs provisioned phone numbers with MSAG addresses. After the selective router identifies the appropriate PSAP for each call, it determines the correct routing path for the call and transmits it, together with the caller's location and telephone number, to the central office serving the PSAP. Finally, the central office transmits the 911 call and associated caller information to the PSAP, typically along dedicated trunk lines. The PSAP validates the caller's location and callback number by querying ANI/ALI databases, and dispatches emergency services to the identified location.[39]

NG911 Networks

As part of the broader IP transition, 911 Authorities are deploying new, IP-based NG911

---

[37] *Derecho Report* at 12.
[38] *911 Reliability Order*, 28 FCC Rcd at 17478-79, paras. 7-8; *NG911 Reliability FNPRM*, 40 FCC Rcd at 2680-81, para. 30. *See also* Appendix B.
[39] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2680-81, para. 30.

networks to receive, process, and deliver 911 traffic to PSAPs, and OSPs are changing how they transmit 911 traffic to those networks.[40] At the core of NG911 networks are ESInets that receive and process 911 traffic from OSPs and forward that traffic to PSAPs. 911 traffic enters the ESInet at one or more points of interconnection (POIs). When 911 Authorities designate a POI under our NG911 transition framework, it is called an "NG911 Delivery Point."[41]

OSP IP infrastructure. To reach the POI, OSPs may connect directly in IP or convert their TDM legacy 911 voice traffic to an IP format using an LNG.[42] In some cases, OSPs may contract with third parties providing high-capacity IP-based fiber networks to carry 911 traffic to an ESInet's POI.[43] This traffic may be combined with other telecommunications traffic over major IP transport, or it may be segregated and combined with 911 traffic from other OSPs over 911-specific IP traffic aggregation facilities. OSPs use LISs[44] to store and manage customer location information and records, replacing functions of ANI/ALI databases.[45]

NG911 network infrastructure. ESInets process 911 traffic through a series of interconnected NG911 Core Services (NGCS) that collectively replace the caller location and routing functions of selective routers, ANI/ALI databases, and the MSAG in legacy 911 networks.[46] These services typically include Location Validation Functions (LVFs), Emergency Call Routing Functions (ECRFs), and related technologies that enable the real-time provision of 911 caller location information to PSAPs (together, NGCS Location Facilities).[47] The LVF is a server that validates civic location information against a Geographic Information System (GIS)

---

[40] *NG911 Transition Order*, 39 FCC Rcd at 8152, para. 28.
[41] 47 CFR § 9.28.
[42] *NG911 Transition Order*, 39 FCC Rcd at 8171, para. 71.
[43] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2687, para. 48.
[44] A LIS is a functional element that provides locations of endpoints. A LIS can provide Location-by-Reference or Location-by-Value, and, if the latter, in geodetic or civic forms. A LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. 47 CFR § 9.28.
[45] *NG911 Transition Order*, 39 FCC Rcd at 8179-80, para. 86.
[46] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2680-83, paras. 29-32; *NG911 Transition Order*, 39 FCC Rcd at 8179, para. 86. The Border Control Function (BCF) acts as a firewall between the ESInet and external networks. *NG911 Reliability FNPRM*, 40 FCC Rcd at 2682, para. 31 & n.84.
[47] NGCS location facilities are NG911 IP facilities connected to an ESInet that enable the real-time provision of 911 caller location information to the PSAPs, including but not limited to the Emergency Call Routing Function (ECRF), the Location Validation Function (LVF), and successor technologies. Appendix A (§ 9.19(a)(14), defining "NGCS location facilities"); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2681-82, para. 31.

database to deliver more dynamic and actionable information about a caller's location than legacy ALI/ANI databases can, and the ECRF is a database function that determines the appropriate destination PSAP by mapping the caller's validated location within the boundaries of emergency response zones.[48] NGCS also include Emergency Services Routing Proxies (ESRPs), Policy Routing Functions (PRFs), and other technologies that enable the real-time routing, delivery, and transfer of 911 traffic to PSAPs along with callback information and other associated data (together, NGCS Routing Facilities).[49] The ESRP is a routing engine that queries the ECRF and routes the traffic to the geographically appropriate PSAP in accordance with the PRF, which is the rule set that decides how traffic should be routed based on predetermined policies (e.g., priority levels, time of day, and load balancing).[50]

NG911 networks also may connect with ESInets in other states or with other ESInets serving different regions in the same state. ESInet interconnecting facilities act as bridges between ESInets and support the rerouting of 911 traffic in the event of outages, which enhances the overall resiliency of the NG911 ecosystem across the interconnected service areas.[51]

Transitional NG911 Networks

While nationwide end-state NG911 remains the Commission's goal, it is necessary to recognize and accommodate intermediate architectures during the nationwide transition to NG911. The commonly-accepted transition path for NG911 envisions that NG911 will reach a mature "end state" after all PSAPs have migrated from legacy E911 systems based on TDM circuit-switched telephony to all-IP systems that operate over ESInets and provide the full array

---

[48] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2681-82, para. 31. GIS is a mapping system that collects, stores, and analyzes spatial data, ensuring that emergency services can pinpoint where to send help. *Id*. *See also* 47 CFR § 9.28 ("Location Validation Function").

[49] NGCS routing facilities are NG911 IP facilities connected to an ESInet that enable the real-time routing, delivery, or transfer of 911 traffic to the PSAPs along with callback information and other associated data, including but not limited to the Emergency Services Routing Proxy (ESRP), the Policy Routing Function (PRF), and successor technologies. Appendix A (§ 9.19(a)(15), defining "NGCS routing facilities"); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2681-82, para. 31.

[50] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2681-82, para. 31.

[51] *Id.* at 2689-90, paras. 54-55.

of NGCS.[52] Achieving end-state NG911 will take time, and transitional NG911 networks need significant intermediate and transitional mechanisms in the interim. Transitional NG911 networks blend some legacy network components with IP-based infrastructure while the transition to end-state NG911 is still ongoing. Consequently, such deployments may retain selective routers, ANI/ALI, and other legacy elements as part of the call path even while implementing ESInets and NGCS. Transitional NG911 deployments also typically include gateway facilities that translate 911 traffic between TDM and IP formats as needed, including LNGs, emergency services gateways (ESGWs), legacy selective router gateways (LSRGs), and legacy PSAP gateways (LPGs).[53]

In this *Order*, we modernize our 911 reliability framework for NG911 networks.[54] We seek to ensure that entities essential to delivering emergency calls in the NG911 environment implement common sense reliability measures to minimize risk of 911 outages, particularly catastrophic multi-state outages. To this end, we clarify and expand the CSP definition to identify which entities in the NG911 environment fall under the Commission's 911 reliability framework; update the reliability standards to reflect the capabilities and architectures of IP networks; adopt a definition for interoperability specifically tailored to NG911; and improve oversight processes available to the Bureau and 911 Authorities. The purpose of these actions is to ensure the continued resiliency, reliability, interoperability, and accessibility of the NG911 ecosystem.

Today's *Order* also eliminates the annual certification requirement for 911 reliability that the Commission imposed in 2013. Going forward, we establish a streamlined filing process in which CSPs will submit a one-time reliability certification subject to updates only in the event of

---

[52] NENA: The 9-1-1 Association (NENA), NENA i3 Standard for Next Generation 9-1-1 at 2 (Oct. 7, 2021), https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-STA-010.3e-2021_i3_Stan.pdf (*NENA i3 Standard*); Task Force on Optimal PSAP Architecture (TFOPA), An FCC Federal Advisory Committee, Adopted Final Report at 17, 37-38, 138 (2016), https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf (*TFOPA Final Report*).

[53] *NENA i3 Standard* at 3.

[54] In today's *Order*, "NG911 networks" refers to both transitional NG911 and end-state NG911 networks and ecosystems unless otherwise specified.

material changes. This revised approach recalibrates our 911 reliability framework to focus on critical aspects of the NG911 transition while reducing regulatory burdens. The new certification process will allow CSPs to certify to reliability at the network level on a per-state basis and will no longer require submission of detailed site-based data for thousands of different facilities. These changes will substantially lighten the burden of previous compliance measures in place since 2013 and will enable providers to redirect those resources to implementing reliable networks for the transmission of NG911 traffic.[55]

Development of 911 Network Reliability Practices

The required NG911 reliability practices we adopt today are based on two decades of investigations by the Commission into major network outages, studies and recommendations by federal advisory committees, rulemakings, and ongoing collaboration with industry stakeholders. For example, the Bureau found during its investigation into widespread 911 outages caused by the 2012 derecho that several reliability measures available to NG911 networks—including IP routers with automatic fail-over capability, diverse IP paths to PSAPs, interoperability between PSAPs, and diverse network monitoring—"likely could have significantly lessened the derecho's impact on emergency communications."[56] In 2018, following its investigation into several major network outages, PSHSB identified increased monitoring of 911 network components and faster failovers to redundant network equipment as key mitigating measures.[57] And in 2020, following another series of major communications outages affecting 911, the Bureau encouraged CSPs to follow industry best practices for network reliability including circuit diversity and auditing, rerouting capabilities, and active network monitoring.[58]

---

[55] Exec. Order No. 14,192, § 1, Unleashing Prosperity Through Deregulation, 90 Fed. Reg. 9065, 9065 (Feb. 6, 2025).
[56] *Derecho Report* at 44.
[57] See *Public Safety and Homeland Security Bureau Encourages Communications Service Providers to Follow Best Practices to Help Ensure Network Reliability*, Public Notice, 33 FCC Rcd 3776 (PSHSB 2018). The Bureau also created a new network reliability page (http://www.fcc.gov/network-reliability-resources) to help ensure that network providers, public safety entities, and the general public can readily access the Bureau's work promoting industry best practices. *Id.* at 3776.
[58] *See Public Safety and Homeland Security Bureau Encourages Communications Service Providers to Implement Important Network Reliability Practices*, PS Docket Nos. 11-60 and 20-183, Public Notice, 35 FCC Rcd 13179 (PSHSB 2020) (*2020 Best Practices Public Notice*).

CSRIC regularly advises the Commission on ways to ensure the security, reliability, and interoperability of communications systems and to safeguard 911 service. In 2019, CSRIC VI provided recommendations to the Commission and to service providers concerning needed improvements to the reliability and resiliency of 911 systems during the transition to NG911.[59] CSRIC based its report on information from a wide variety of sources, including industry subject matter experts, 911 Authorities, public safety groups, CSRIC best practices and other CSRIC efforts, industry documents related to NG911 reliability, and FCC reports.[60] CSRIC recommended, for example, that service providers monitor for events that could result in a loss of service;[61] incorporate network monitoring tools on originating and transport networks specifically, to protect 911 traffic before it reaches the ESInet perimeter;[62] and work with stakeholders to share monitoring information.[63] CSRIC's updated best practices for NG911 included: geographic separation of network redundancy facilities; configuring backup power at critical sites to auto-engage in the event of a failover; development of standards for network interconnections; securing transport over the public Internet with authentication and confidentiality mechanisms such as digital signatures and Virtual Private Network (VPN) tunneling; logical diversity for NG911 signaling networks, confirmed with regular diversity audits; dedicated, geo-diverse, and redundant IP connection points; geographically diverse 911 location servers; functional redundancy and geographic diversity for critical network elements; physical and geographic redundancy for critical facilities links; diverse routing from OSPs to the ESInet; and redundant connectivity from the ESInet to PSAPs.[64]

Separately, the Commission asked CSRIC VII to survey the state of interoperability for the

---

[59] CSRIC VI Working Group 1, Final Report – Recommendations for 9-1-1 System Reliability and Resiliency during the NG9-1-1 Transition; Version 2.0 – March 8, 2019 (Addition of Best Practices) (2019), https://www.fcc.gov/sites/default/files/csric6wg1_finalreport_030819.pdf (*CSRIC VI WG 1 Report*).
[60] *Id.* at 7, 11-14.
[61] *Id.*
[62] *Id.* at 69-70.
[63] *Id.* CSRIC also provided information on commercially-available tools used "to detect, deter and mitigate network anomalies within the 9-1-1 networks infrastructure." *Id.* at 75, Appendix A.
[64] *Id.* at 86, 87, 109, 114, 122, 124.

nation's 911 systems, including for legacy 911 networks, transitional 911 networks, and NG911.[65] CSRIC observed that 911 systems are highly interconnected and that interoperability between call-taking and call processing components is critical.[66] CSRIC concluded that the state of national NG911 interoperability is highly dependent on the degree of progress made by state and local 911 authorities in transitioning their respective systems to mature or end-state NG911 capability.[67] CSRIC identified interoperability challenges and indicators of successful interoperability and recommended that the U.S. "continue to move forward with the deployment of NG9-1-1, with a strong focus on achieving interoperability, as defined in this report, which includes industry standards-based solutions."[68]

The Need for Changes to the 911 Reliability Framework

NG911 provides significant advantages over legacy 911 systems, including enhanced reliability, redundancy, interoperability, and accessibility. However, without robust design, NG911 networks can heighten the risk to the public of widespread outages due to their increased aggregation and consolidation of traffic. In contrast to legacy 911 networks, in which call origination, routing, and delivery occur locally and are managed by a small set of providers, the NG911 ecosystem typically aggregates traffic from OSPs across broad geographic regions, transports this traffic over long distances, and relies on multiple operators. This aggregation makes the NG911 ecosystem more capable and flexible but also larger and more complex than

---

[65] CSRIC VII, Working Group 4, Report on the Current State of Interoperability in the Nation's 911 Systems (2020), https://www.fcc.gov/CSRICReports (*CSRIC VII WG 4 Report*).
[66] *Id.* at 5.
[67] *Id.* at 22-23. CSRIC utilized the "maturity states" defined by the FCC's earlier TFOPA in crafting its report formulation. *See* TFOPA, Working Group 2, Phase II Supplemental Report: NG9-1-1 Readiness Scorecard at 13 (Dec. 2, 2016), https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_Supplemental_Report-120216.pdf. (*TFOPA Scorecard*). The scorecard defined states of transition ranging from legacy state, through foundational, transitional, and intermediate states, culminating in the jurisdictional and nation-wide "end state" of NG9-1-1 service. Per TFOPA, "End State" refers to the state in which PSAPs have evolved to become emergency communications centers (ECCs) and are served by standards-based NG911 systems and/or elements and OSPs are providing SIP interfaces with location information during call setup, and ESInets are interconnected providing interoperability on a national basis, supported by established agreements, policies and procedures. *See also* James Careless, *PSAP & Emergency Communications Centers Explained*, Public Safety Broadband Technology Association (Jun. 16, 2025), https://thepsbta.org/psap-emergency-communications-centers-explained-psbta/ ("[A]n ECC performs the 911 call center functions of a PSAP, but can offer additional capabilities as well. For instance, an ECC can handle non-emergency calls, assist in coordinating responses to multiple emergencies, and manage multi-agency communications during large-scale incidents.").
[68] *CSRIC VII WG 4 Report* at 25.

the legacy ecosystem, with higher traffic volumes carried over longer transport paths than in legacy networks. Additionally, as noted above, the transitional NG911 ecosystem depends on functional elements that translate 911 calls between TDM and IP formats—elements often located far from the point where calls originate or are handed off to ESInets and PSAPs. The risks posed by substandard implementation of this new network architecture are not theoretical, as evidenced by recent 911 outages attributable to vulnerabilities in heretofore unregulated network elements.[69] As NG911 deployment accelerates, close coordination between industry, public safety entities, 911 Authorities, and the Commission is essential to ensure against vulnerabilities that could undermine 911 reliability, resiliency, and accessibility.

Alongside the broader IP transition, the emergence of NG911 has given rise to new classes of service providers that did not exist in legacy 911 networks but play essential roles in the NG911 ecosystem's call path. These new provider classes include third-party transport providers retained by OSPs to carry 911 traffic over high-capacity fiber networks; specialized entities that aggregate 911-only traffic for transport and delivery; and providers of IP-based signaling translation functions.[70] NG911 network providers frequently engage third-party operators to manage servers and other critical facilities supporting 911 call routing and other key functions across multiple states and jurisdictions.[71] Some of these new providers are not covered by the Commission's previous 911 reliability rules, despite their essential and expanding role in

---

[69] *See*, *e.g.*, New York Public Service Commission (NYPSC) Comments at 2 (attesting to widespread 911 outages in New York originating in major transport networks that "took significantly longer to identify and understand" because the networks were not covered by the 911 reliability rules); NENA Comments at 1-2 (reporting that "failures downstream of the [OSP] but upstream of the [ESInet]" have been the cause for "several states that have had repeated widespread outages" resulting in "wide swaths of the state [being] unable to place 9-1-1 calls"); Colorado Council of Authorities, Inc. (CCOA) Comments at 2 (stating that unregulated "aggregators and operators of high-capacity transport facilities" have been the source of recent vulnerabilities, which "disrupts critical 911 functions and impacts multiple" PSAPs); Colorado Public Utilities Commission (COPUC) Comments at 2; Brian Rosen Comments at 3. *See also NG911 Reliability FNPRM* at 2676-77, paras. 16-18.

[70] *See* Letter from Frank Pozniak, Executive Director, Massachusetts State 911 Department, to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 21-479, 13-75, at 2-3 (filed Jun. 18, 2026) (*Massachusetts Ex Parte*) (endorsing inclusion of third-party 911 service providers as CSPs based on Massachusetts' experience that most OSPs are heavily reliant on CSPs in NG911).

[71] FCC Public Safety and Homeland Security Bureau, April 2014 Multistate 911 Outage: Cause and Impact, PS Docket No. 14-72 at 1-2 (2014), https://www.fcc.gov/document/april-2014-multistate-911-outage-report.

maintaining the continuity of 911 service.[72] Other NG911 capabilities fall within the category of "functional equivalents" under the prior rules, yet, as we detail below, the record demonstrates that many new providers of these capabilities have not recognized that the prior rules apply to them. Moreover, the prior reliability rules are inherently static, such that tethering NG911 "functional equivalents" to the legacy environment does not allow the rules to scale effectively to accommodate the continued evolution of IP-based NG911 call-originating technologies and exchanges of information. Without clarifying the 911 reliability framework to expressly cover all critical NG911 providers and functions, the Commission cannot effectively address or mitigate the risks of significant outages on IP-based and NG911 networks.[73]

As the Commission observed in the *NG911 Reliability FNPRM*, the landscape of 911 outage risk has evolved significantly since 2013. The *FNPRM* specifically cited examples of major 911 outages affecting millions of Americans in multiple states as 911 Authorities seek to transition from legacy 911 to NG911.[74] Moreover, since the release of the *FNPRM*, additional 911 outages have occurred in Pennsylvania, Mississippi, Louisiana, Alabama, Wyoming, and Montana, highlighting continued vulnerabilities that can affect statewide and multi-state NG911 deployments.[75] Some of these outages were triggered by single fiber cuts, which indicates that NG911 networks have not yet consistently implemented the geographically-distributed reliability

---

[72] NENA Comments at 1-2; COPUC Comments at 2. One of the 911 aggregation service providers has "deployments of NG911 call aggregation service in states and counties across the country" and claims to serve over 30% of the U.S. population. Sinch, *Inteliquent exceeds 30% of population with recent next generation call aggregation deployments*, https://sinch.com/news/ng911-call-aggregator-inteliquent-leads-us-public-safety/?UTM-Inteliquent (last visited May 19, 2026) (Sinch acquired Inteliquent in 2021.); Sinch, *Bring public safety to the digital age with NG911*, https://sinch.com/voice/next-generation-911/ (last visited May 19, 2026).

[73] *See* COPUC Comments at 4; NENA Comments at 1-3; National Association of State 911 Administrators (NASNA) Comments at 1-2. *See also* 47 CFR § 9.19(4)(i).

[74] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2676-77, paras. 16-17.

[75] Meir Rinde, *Pennsylvania's 911 service experiencing statewide outage* (Jul. 11, 2025), https://whyy.org/articles/pennsylvania-911-calls-philadelphia-emergency-response/; *911 emergency lines restored in Mississippi, still down in parts of Louisiana* (Sept. 25, 2025), https://www.cbsnews.com/news/911-emergency-lines-down-mississippi-louisiana/; *AT&T Attributes Mass 911 Outages in 3 States to Fiber Cuts Made by 'Third Parties'* (Sept. 26, 2025), https://www.usnews.com/news/best-states/mississippi/articles/2025-09-26/at-t-attributes-mass-911-outages-in-3-states-to-fiber-cuts-made-by-third-parties; Renée Jean, *Broken Fiber Line In Park County Exposes Fragility In Wyoming's 911 System* (Jan. 7, 2026), https://cowboystatedaily.com/2026/01/07/broken-fiber-line-in-park-county-exposes-fragility-in-wyomings-911-system/; Jenn Rowell, *Fiber Optic Line Maintenance Causes 911 Outage in Cascade County*, The Electric (Mar. 4, 2026), https://theelectricgf.com/2026/03/04/fiber-optic-line-maintenance-causes-911-outage-in-cascade-county/.

measures we adopt in our *Order* today. Several failures originated in portions of the NG911 call flow located downstream of originating providers' owned-and-operated networks but upstream of ESInet and NGCS elements covered as "functional equivalents" under the 2013 reliability rules.[76] Failures in these uncovered transport and aggregation segments can interrupt 911 service to dozens or hundreds of PSAPs, yet, to date, both the Commission and 911 Authorities have lacked visibility into the reliability practices employed by providers operating in this segment.[77] Without remedial action, these vulnerabilities could contribute to the continued occurrence of major "sunny day" 911 outages.[78]

The framework we adopt today is narrowly tailored to strengthen NG911 networks while eliminating unnecessary regulatory burdens. By eliminating the requirement that CSPs file annual certifications and replacing it with a streamlined certification process, we maintain accountability while reducing the administrative burden on CSPs. We further align this streamlined regulatory oversight with the actual flow of 911 traffic in NG911 networks to ensure the rules remain appropriately limited to demonstrated areas of vulnerability. Our updated definition of "covered 911 service provider" focuses on those entities that play essential roles in routing, validating, or transporting 911 traffic in real time and whose failure would pose the most significant risk to service availability. Our updated reliability benchmarks address the principal vulnerabilities in NG911 architecture without imposing unnecessary or overly prescriptive requirements on CSPs. These benchmarks incorporate reliability measures recommended by CSRIC and recognized in the record as prevailing best practices, while also leveraging the inherent strengths of IP-based systems to adapt and self-heal in real time.[79] The new framework

---

[76] The Commission requires certain OSPs to transmit 911 calls with appropriate location information to a PSAP, to a designated statewide default answering point, or to an appropriate local emergency authority. 47 CFR §§ 9.4, 9.8, 9.10, 9.11, 9.14, 9.18. Under the Commission's NG911 transition framework, OSPs also have the obligation to deliver 911 traffic to the NG911 delivery point, which is a logical demarcation dividing the responsibilities of OSPs and 911 Authorities for the delivery of 911 traffic. *See* 47 CFR §§ 9.29, 9.32, 9.33.

[77] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2676-77, paras. 16-18.

[78] *See 2014 911 Reliability NPRM*, 29 FCC Rcd at 14222, para. 32 (noting that the 2013 rules may need to be updated to address changes in 911 technologies and the persistence of "sunny day" 911 outages).

[79] *NG911 Transition Order*, 39 FCC Rcd at 8222, para. 186 & n.546. (citing Intrado's assertion that "establishing direct OSP connectivity via SIP to ESInets 'will materially reduce the number of 911 outages through improved network reliability and availability'"). *See also*, *e.g.*, StateScoop*, North Carolina officials say next-generation 911*

will optimize NG911 to meet operational needs today and tomorrow and ensure that actionable location and call back information and other data reliably move from callers to PSAPs and enable PSAPs to dispatch emergency responders quickly and effectively.

The record also underscores the importance of updating our 911 reliability framework now, while the NG911 transition is still in a relatively formative phase, rather than waiting for further NG911 deployments or full completion of the transition.[80] We agree with 911 Authorities, national public safety organizations, and some OSPs that an orderly transition to the NG911 ecosystem requires prompt updating of the definition of CSPs and the 911 reliability standards.[81] We disagree with industry commenters who argue that such action is premature.[82] We conclude that waiting until the transition is completed to see what problems remain to be addressed ignores demonstrated risks to 911 reliability and needlessly delays implementation of available solutions.[83] The stakeholder community has already developed detailed and well-established technical architecture and commonly accepted standards for NG911 systems,[84] and the reliability framework we adopt today is based on well-documented best practices for IP networks that can readily be implemented by CSPs as part of their network build-outs.

---

network withstood Hurricane Helene (October 21, 2024), https://statescoop.com/north-carolina-next-generation-911-hurricane-helene/ ("Had the old technology and analog network still been in place, the infrastructure would have been destroyed and we would not have had the capability to route calls to other PSAPs and connect people to critical emergency services . . . . Thanks to the resiliency and redundancy of this network, we had no reports of 911 calls not being delivered.").

[80] Association of Public-Safety Communications Officials, International (APCO) Reply at 14-15; COPUC Comments at 1-2.

[81] *See*, *e.g.*, NYSPSC Comments at 1-2; Texas 9-1-1 Entities Comments at 2-3; COPUC Comments at 1-2; Michigan State 911 Committee Comments at 1; Colorado Council of Authorities, Inc. (CCOA) Reply at 2-3; NASNA Comments at 1; NENA Comments at 1; APCO Reply at 14-15; Palmetto Broadband Coalition Reply at 3; Home Telephone ILEC, LLC (Home Telephone) Comments at 11. *See also* Public Knowledge Comments at 4.

[82] Lumen Comments at 2. *See also* Intrado Life & Safety, Inc. (Intrado) Comments at 1-2, 16-17; USTelecom – The Broadband Association (USTelecom) Comments at 2-4; Bandwidth Inc. and Bandwidth.com (Bandwidth) Comments at 1-2; NCTA - The Internet and Television Association (NCTA) Comments, PS Docket No. 21-479, WC Docket Nos. 04-36, 10-90, 17-97, GN Docket No. 13-5 at 2-3 (rec. Jun. 11, 2025) (NCTA Comments); Intrado Reply at 2-3; Industry Council for Emergency Response Technologies (iCERT) Reply at 2; Comtech Telecommunications Corp. (Comtech) Reply at 4-5.

[83] Lumen Comments at 2; iCERT Reply at 2.

[84] *See TFOPA Final Report*; *NENA i3 Standard.* In July 2021, NENA released the third version of the i3 standard for NG911. NENA, NENA Releases New Version of the i3 Standard for Next Generation 9-1-1 (July 12, 2021) https://www.nena.org/news/572966/NENAReleases-New-Version-of-the-i3-Standard-for-Next-Generation-9-1-1.htm. In October 2021, the NENA i3 standard was approved by the American National Standards Institute (ANSI). NENA, ANSI Approves NENA's i3 Standard for Next Generation 9-1-1 (Oct. 7, 2021), https://www.nena.org/news/582667/ANSI-Approves-NENAs-i3- Standard-for-Next-Generation-9-1-1.htm.

Concurrently, many 911 Authorities have initiated the implementation of NG911 functional elements, made substantial investments in NG911 systems (spending over $500 million on NG911 programs in 2024 alone),[85] and submitted valid requests for NG911 service covering a significant portion of the United States. These collective efforts demonstrate that the NG911 ecosystem has reached a level of maturity where uniform expectations for reliability are both feasible and necessary. These efforts have also provided us with ample guidance to modernize the reliability framework in a way that reflects current operational realities and keeps pace with the fast-moving technological evolution of the capabilities inherent in IP-based networks. Adopting an updated framework now ensures that NG911 networks will be designed according to reasonable reliability standards from the outset and avoids the need for inefficient and costly retrofits in the future.[86] Early action also provides 911 Authorities with tools to engage in appropriate oversight of newly deployed NG911 services, enabling more effective planning and management of subsequent system performance and resiliency.[87] We revise our oversight framework in a streamlined manner, ensuring transparency and accountability while minimizing burdens and protecting sensitive operational information. In addition, we are providing an 18-month transition period for implementation of the new framework to afford CSPs time to integrate the updated reliability benchmarks into their ongoing NG911 deployments and to refine their networks, operations, and reliability practices accordingly. These actions reaffirm our commitment to ensuring that 911 remains dependable, resilient, and available when Americans need it most.

911 Reliability

Covered 911 Service Providers

As proposed in the *NG911 Reliability FNPRM*, we update the definition of "covered 911

[85] *Seventeenth Annual 911 Fee Report* at 3.
[86] *See*, *e.g.*, APCO Reply at 14 ("[R]eliability measures must be built into these systems from the outset."); COPUC Comments at 1-2; NASNA Comments at 1-2.
[87] NASNA Comments at 6 ("CSPs should not be permitted under the rules to omit critical functional elements during procurement and then lay the responsibility at the feet of the local 911 jurisdiction citing *caveat emptor*."); NYSPSC Comments at 2.

service provider" to accurately reflect the modern NG911 ecosystem and ensure that providers of critical NG911 services design their networks to safeguard 911 traffic.[88] We preserve the reliability requirements for legacy covered 911 services while more specifically defining the NG911 routing and location capabilities covered as part of this definition. We do this by clarifying that NGCS that provide NG911 location and routing capabilities are the "functional equivalent" of legacy selective routing and ANI/ALI services. We also expand the covered 911 services definition to include transport and aggregation facilities carrying substantial 911 traffic from two or more OSPs as well as some other shared facilities. These actions ensure that the term "covered 911 service provider" encompasses entities providing 911, E911, or NG911 services for which a failure would impede the real-time routing, delivery, or transfer of 911 traffic.[89]

While the transition to NG911 is progressing alongside broader IP modernization, 911 Authorities and OSPs will continue for some time to rely on legacy selective routers and other TDM-based infrastructure for delivery of 911 calls to PSAPs.[90] In transitional NG911 systems, these legacy 911 network elements (selective routers; ANI/ALI databases; and TDM 911 circuits between selective routers, ALI/ANI databases, and the last central office serving a PSAP) will be treated as covered 911 facilities as they were under the 2013 reliability rules.[91] NGCS facilities

---

[88] Appendix A (§ 9.19(a)(4)).

[89] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2686-2687, 2689, paras. 44-45, 53.

[90] *Reducing Barriers to Network Improvements and Service Changes*; *Accelerating Network Modernization*, WC Docket Nos. 25-209 and 25-208, Report and Order, FCC 26-19, 2026 WL 1016892 (Mar. 27, 2026). The Commission's goal during this period is to encourage the development and deployment of advanced IP networks and services, including NG911, while ensuring seamless 911 connectivity. *Id*. at *25, para. 69. To that end, among other protections, the Commission requires carriers seeking to discontinue services supporting interconnection trunks or exchange of traffic to provide impacted 911 Authorities, 911 service providers defined as an entity that provides 911, E911, or NG911 capabilities or the functional equivalent of those capabilities directly to a PSAP, and directly interconnecting local exchange service providers that support essential functions within 911 networks with advance notice and a point of contact with which to coordinate an orderly transition away from legacy facilities that support 911. *Id*. at *24-25, paras. 67, 69 ("[W]e expect that carriers and service providers will engage in a planned and managed process for the orderly shutdown or reduction of services to . . . 911 Authorities handling live traffic, while ensuring compliance with regulatory requirements and a smooth transition to alternative providers.").

[91] Appendix B provides three illustrative network diagrams that demonstrate the application of our updated 911 reliability framework for legacy and transitional environments as well as for more mature NG911 configurations. The diagrams include an overlay of the presumptive cost allocation between OSPs and 911. Historically, the Commission has found that OSPs should bear the costs associated with transmitting legacy 911 calls from their end users to the points where they hand off such calls to selective routers used to transmit those calls to appropriate PSAPs. *NG911 Transition Order*, 39 FCC Rcd at 8202-03, para. 146 (citing *Revision of the Commission's Rules to*

and ESInet IP paths to PSAPs will also be covered 911 facilities, as will ESInet paths between NG911 delivery points and NGCS facilities. The definition of covered 911 services includes operation of NG911 and transitional elements serving two or more OSPs, such as LNGs, ESGWs, LSRGs, LISs, and LPGs.

In more mature NG911 systems, in which the selective router, legacy ANI/ALI facilities, and covered 911 TDM circuits connecting selective routers are no longer part of the call flow, the updated definition of covered 911 services includes ESInets, NGCS facilities, and ESInet IP covered 911 paths, as well as NGCS routing and location facilities such as the ESRP, PRF, ECRF, and LVF.[92] Covered 911 services also include several multi-OSP services, including IP 911 traffic aggregation, major IP transport, and shared LIS and LNG facilities.[93]

Technologically neutral regulation of 911 reliability. Historically, the Commission has allowed providers to use various proven technologies and approaches to comply with 911 reliability rules rather than prescribing specific solutions.[94] We reaffirm this commitment to a technologically neutral approach for regulating covered 911 providers in order to "future-proof" our framework, an approach that is strongly supported by commenters in this proceeding and will provide regulated entities compliance flexibility. Consistent with this principle, we define a CSP as any entity that provides 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.[95] This definition uses informative, non-normative examples,[96] with reference to functional elements

---

Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Request of King County, Washington, CC Docket No. 94-102, Order on Reconsideration, 17 FCC Rcd 14789 (2002)). Under the Commission's NG911 transition framework, OSPs similarly are financially responsible for the costs of transmitting 911 traffic from their end users to NG911 Delivery Points, in the absence of an alternative cost arrangement with the relevant 911 Authority. *Id.* at 8201-06, paras. 145-153.

[92] *See* Appendix B.

[93] *See id*. (Figure 3 also shows LPGs and interstate interconnecting ESInet facilities as covered 911 services).

[94] *See*, *e.g.*, *NG911 Transition Order*, 39 FCC Rcd at 8159-60, paras. 39-40.

[95] USTelecom Comments at 6 ("USTelecom recommends that the Commission define CSPs based on core NG911 functionalities—namely, whether a service enables the selective routing or delivery of 911 calls or the associated transmission of caller location and call-back information."); iCERT Comments at 7 (stating the FCC's CSP definition "should cover providers that enable the real-time routing, delivery, or transfer of 911 calls or texts, along with location or callback information, and other associated data (collectively, the 'NG911 Core Functions'), rather than stipulating whether a particular service falls into a predefined category"). Appendix A (§ 9.19(a)(4)(i)).

[96] ATIS Reply at 3.

featured in current commonly accepted NG911 standards, in order to clearly delineate the types of services that are critical to 911 reliability today. Our technologically-neutral approach also serves to ensure that we do not "inadvertently stifle innovation, create misalignment with standards-based implementations, or sweep in entities whose operations do not materially impact the delivery of emergency services."[97] We believe that our approach is flexible enough to not only ensure clear compliance today but also to guide future compliance as technologies change.

Preserving State and Local Government Flexibility. Today's action leaves in place the exemption for state and local governments operating their own facilities that would otherwise be covered 911 services. Thus, no PSAP, 911 Authority, or other governmental authority directly providing 911, E911, or NG911 capabilities is a CSP or is otherwise subject to these regulations.[98] Further, we emphasize that we do not preclude states from adopting their own 911 reliability approaches that do not conflict with the Commission's goals in this proceeding, for example, by adopting reliability measures for smaller transport facilities than those we regulate today.[99] In addition, for CSPs that directly serve 911 Authorities, today's framework leaves in place the ability to implement alternative reliability measures to mitigate the risk of failure in certain situations, taking into account the level of service ordered by the PSAP or 911 Authority.[100]

Applicability to OSPs. The Commission requires OSPs—by which we generally mean entities that offer end users the ability to originate 911 calls—to transmit such calls with appropriate location information to a PSAP, to a designated statewide default answering point, or

---

[97] USTelecom Comments at 5. *See also* CTIA Reply at 2-3, 5; Verizon Comments at 3.

[98] We make non-substantive, clarifying edits to the language in section 9.19(a)(4)(ii) setting forth this exemption. The revised rule now specifies that 911 Authorities are exempt governmental authorities and that the 911 capabilities that are exempted include E911 and NG911 capabilities. Appendix A (§ 9.19(a)(4)(ii)(A)).

[99] COPUC Comments at 2 (explaining the Commission's and states' "shared concurrent jurisdiction" over 911, where "the Commission sets a baseline for 911 networks and call delivery and the states add to this through statute, regulation, and service level agreements").

[100] *911 Reliability Order*, 28 FCC Rcd at 17497, para. 62 ("The Bureau will consider a number of factors in determining whether the particular alternative measures are reasonably sufficient to ensure reliable 911 service. Such factors may include the technical characteristics of those measures, the location and geography of the service area, the level of service ordered by the PSAP, and state and local laws (such as zoning and noise ordinances)."). *See also id.* at 17504, 17510, paras. 83, 98.

to an appropriate local emergency authority.[101] As part of the NG911 transition framework, the Commission also requires OSPs to deliver all 911 traffic to NG911 Delivery Points following the receipt of a valid request from a 911 Authority for Phase 1 or 2 service.[102] This *Order* does not alter the scope or applicability of such OSP requirements, nor does it apply 911 CSP reliability requirements to OSPs. However, as discussed below, we revise the 911 reliability framework to address third-party transport and aggregation of 911 traffic from OSPs to NG911 delivery points.

The 911 transmission rules already in place are distinct from the measures to support 911 reliability that we adopt today. As an initial matter, the 911 transmission rules and the 911 reliability framework apply to two different classes of providers. The 911 transmission rules apply to telecommunications carriers and certain other providers that originate 911 traffic, i.e., OSPs. CSPs, on the other hand, provide 911, E911, or NG911 capabilities that do not include call origination.[103] Originators of 911 calls have been explicitly excluded from the 911 reliability framework where another service provider, typically a CSP, transmits the calls to a PSAP.[104] We maintain this exemption while updating it to reflect the reality that, in NG911 networks, 911 traffic is delivered to 911 Authorities at their ESInet POI.[105] However, to fulfill

---

[101] We call the relevant provisions at sections 9.4, 9.8, 9.10, 9.11, 9.14, and 9.18 the "911 transmission rules" in this *Order*. *See* 47 CFR § 9.4 (requiring telecommunications providers to transmit all 911 calls to a PSAP, designated statewide default answering point, or appropriate local emergency authority; rule does not address transmission of location information); 47 CFR § 9.8 (requiring fixed telephony service providers to transmit caller location information with 911 calls); 47 CFR § 9.10(b) (requiring CMRS providers to transmit all wireless 911 calls and provide certain location information to a PSAP, designated statewide default answering point, or appropriate local emergency authority); 47 CFR § 9.11(b)(2)(ii) (requiring interconnected VoIP providers to transmit all 911 calls and provide certain location information to a PSAP, designated statewide default answering point, or appropriate local emergency authority); 47 CFR § 9.14(d)(iii) (requiring VRS and IP relay providers to transmit all 911 calls, certain location information, and other information to a PSAP, designated statewide default answering point, or appropriate local emergency authority); 47 CFR § 9.14(e) (requiring IP CTS providers to transmit all 911 calls, certain location information, and other information to a PSAP, designated statewide default answering point, or appropriate local emergency authority); 47 CFR § 9.18(a) (requiring providers of Mobile-Satellite Service to provide Emergency Call Center service, where personnel must "determine the emergency caller's phone number and location and then transfer or otherwise redirect the call to an appropriate public safety answering point").

[102] *See* 47 CFR § 9.28 (defining OSPs); 47 CFR § 9.29(a), (b) (NG911 delivery rules).

[103] 47 CFR § 9.19(a)(4); iCERT Comments at 12 ("While OSPs are responsible for originating 911 calls or texts, they do not perform the core NG911 functions that the Commission has historically tied to CSP obligations, such as the routing, delivery, or location processing of 911 calls and associated data to the appropriate PSAP.").

[104] 47 CFR § 9.19(a)(4)(ii)(b).

[105] Appendix A (§ 9.19(a)(4)(ii)(B)); Letter from Steve Morris, Vice President and Deputy General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 21-479, 13-75, at 2 (filed May 4, 2026) (encouraging the Commission "to clarify that OSPs that contract with third parties for regulated functions are not themselves covered by the new rules.").

their transmission obligations under our rules, OSPs frequently contract with third parties to pick up 911 traffic from their networks and transport it to 911 Authorities' 911 networks.[106] Under the framework adopted in this *Order*, some of these third parties—specifically major IP transport providers and IP 911 traffic aggregators—will now be CSPs.

Some commenters contend that extending the scope of the CSP requirements to entities that contract with OSPs creates a substantial new regulatory burden without a corresponding benefit to 911 systems.[107] We disagree. It is reasonable to assume that OSPs already consider, when selecting transport and aggregation vendors, whether those vendors have implemented reasonable reliability measures in order to support their 911 transmission obligations.[108] Today, we add an additional level of assurance for OSPs if they select an entity providing major IP transport or IP 911 traffic aggregation services, because our new framework now requires these entities to implement basic resiliency and reliability measures. Since these new types of CSPs consolidate enough 911 traffic that an outage affecting them would severely impact the availability of 911 services to the public, ensuring that these entities implement basic reliability measures is a reasonable step. Additionally, extending reliability requirements to these new types of CSPs supports the ability of OSPs to fulfill their 911 transmission obligations.

For these reasons, we disagree with comments contending that our amendments to section 9.19 will duplicate obligations that OSPs already have under the 911 transmission rules and that the 911 transmission rules are sufficient to ensure reliability on the OSP side of the NG911 call

---

[106] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2677, para. 17. OSPs may, as an alternative, directly connect to 911 networks. *Id.*

[107] Lumen Reply at 2 & n.5; USTelecom Comments at 6 ("[B]ecause [OSPs] are further away from PSAPs than entities currently falling within the definition of a CSP, they have less direct control over public safety outcomes[.]").

[108] *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, PS Docket No. 15-80, Order on Reconsideration, 39 FCC Rcd 7362, 7368, para. 14 (2024) (*911 Outage Notification Recon. Order*) (noting "long-held Commission precedent that licensees and other regulatees are responsible for the acts and omissions of their contractors, and that it does not serve the public interest to create a means for OSPs to 'contract away' their obligations"); 47 U.S.C. § 217 ("[T]he act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person."); *Lumen Technologies*, Notice of Apparent Liability for Forfeiture, 38 FCC Rcd 9750, 9752, para. 8 (2023).

path.[109] In reality, our updated reliability framework empowers the Commission to apply its 911 oversight authority preventatively to facilities instead of after an outage when transmission rule violations have already occurred. Moreover, as discussed in greater detail below, we have addressed these commenters' concerns by adjusting the proposed definitions of the newly-covered CSP facilities so that they apply exclusively to high-volume, third-party services provided to two or more OSPs and not to transmission capabilities that OSPs provide via their own networks. Far from imposing duplicative burdens on OSPs, our amendments to section 9.19 provide greater certainty for OSPs that contract with third-party CSPs to provide 911 transport or delivery services. OSPs will now be able to easily assess the reliability of these service providers based on their implementation of the Commission's requirement to provide reasonably reliable 911 services.

NG911 cost allocation. In legacy 911 networks, ILECs operate most or all of the network infrastructure used to route and deliver 911 calls to PSAPs under tariff or contractual agreement with PSAPs and emergency authorities.[110] When the Commission adopted the 2013 reliability rules, these tariff and contractual arrangements were well-established, so the Commission did not address cost issues at that time. Instead, the Commission focused on enhancing the reliability of the 911 capabilities being provided through these relationships.[111] When the Commission established its NG911 Transition framework in 2024, it found it necessary to expressly allocate NG911 costs between OSPs and 911 Authorities, because uncertainty and disagreements over the basic terms on which OSPs would begin to provide NG911 service were delaying the nationwide transition to NG911.[112] Under the NG911 Transition framework, OSPs are presumptively responsible for the costs of translating 911 traffic into SIP format and the costs of delivering 911 traffic and associated routing and location information to the NG911 Delivery

---

[109] *See* Verizon Comments at 9; iCERT Reply at 5 (urging the Commission not to impose overlapping, duplicative requirements between OSPs and CSPs); CTIA Comments at 2-4; T-Mobile Comments at 2-4.
[110] *2014 911 Reliability NPRM*, 29 FCC Rcd at 14214, para. 16.
[111] *See generally* 47 CFR § 9.19(a)(4) (defining CSPs as entities that directly serve PSAPs).
[112] *NG911 Transition Order*, 39 FCC Rcd at 8197, para. 134.

Points designated by 911 Authorities.[113] In other words, OSPs are "responsible for the costs of complying with their own 911 service obligations,"[114] while 911 Authorities bear the costs incurred beyond NG911 Delivery points to process and transmit 911 traffic to the appropriate PSAP.[115] OSPs and 911 Authorities may, however, modify these default cost allocations by mutual agreement.[116]

As the national transition to IP-based telecommunications has advanced and NG911 network architectures have evolved, the array of entities providing 911 capabilities has become more complex. The contractual arrangements through which NG911 service is provided have become more complex as well. For example, we identify today several new classes of IP-based CSPs that have become essential to the routing and delivery of 911 traffic in the NG911 environment. Among them are CSPs that provide processing and transport of 911 traffic from OSPs' networks to NG911 Delivery Points or ESInet POIs. These entities often have contractual relationships with OSPs rather than direct relationships with PSAPs or 911 Authorities. Several commenters question which entities should bear the costs of newly designated CSP services in the NG911 environment.[117] We therefore clarify that nothing in this *Order* changes the default cost allocation the Commission adopted in the *NG911 Transition Order*. OSPs remain presumptively responsible for costs of delivery to the NG911 Delivery Point or other ESInet POI, regardless of whether they deliver traffic entirely over their own networks or hire third-party CSPs to provide intermediate transport and/or aggregation.[118] 911 Authorities remain

---

[113] *Id.* at 8196, para. 132.
[114] *Id.* at 8202-03, para. 146 (noting that making OSPs responsible for the cost of meeting their service obligations "is analogous to the cost requirement the Commission adopted over two decades ago during the implementation of wireless E911") (citing *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*; *Request of King County, Washington*, CC Docket No. 94-102, Order on Reconsideration, 17 FCC Rcd 14789, 14789, 14792-93, paras. 1, 8-10 (2002)).
[115] *NG911 Transition Order*, 39 FCC Rcd at 8196, para. 132.
[116] *Id*. at 8180, para. 87; 47 CFR § 9.34.
[117] *See*, *e.g.*, NTCA and the RLEC Parties Comments at 4-5 ("[T]he Commission should reaffirm the carriers' relative responsibilities for the costs they will incur under the new NG911 regime . . . and specifically clarify that state 911 [A]uthorities and NG911 [CSPs] cannot pass on to OSPs any compliance costs the former assume associated with the adoption of the proposed reliability framework."); USTelecom Reply at 4-6 (requesting clear distinctions between OSPs and CSPs to avoid unfair cost burdens); Intrado Comments at 16-17.
[118] *NG911 Transition Order*, 39 FCC Rcd at 8196, 8202-03, paras. 132, 146.

presumptively responsible for completing 911 calls after they are handed off at the NG911 Delivery Point and therefore bear the costs of ESInets, NGCS, and other NG911-related CSP services beyond that point.[119] We emphasize, however, that the framework's division of cost responsibilities is not prescriptive, and 911 Authorities and OSPs may agree to alternative cost structures.[120]

NG911 Functional Equivalents

As proposed in the *NG911 Reliability FNPRM*, we define NG911 location and routing capabilities that are part of NGCS as covered 911 services because they are the functional equivalents of legacy selective routing and ANI/ALI services that were identified as covered services under the original CSP definition.[121] The Commission adopted the "functional equivalent" language in 2013 to ensure that the CSP definition would be flexible enough to capture emerging NG911 entities while avoiding overbroad regulation.[122] While this approach has been effective to a degree, the recent acceleration of the NG911 transition requires us to provide additional clarity to aid in compliance with 911 reliability framework. NENA points out that some companies operating critical NG911 facilities have argued the "functional equivalent" language in the 2013 rules does not include their facilities, and so no specific reliability measures are required.[123] CCOA also cites a service provider that has argued the original circuit diversity rules only apply to circuits from routing facilities in central offices and not to critical circuits elsewhere in the 911 call path.[124]

To address these concerns, we reference specific NGCS location and routing functions to make the updated 911 reliability framework clearly applicable to critical NGCS services and facilities.[125] We define NGCS location facilities as functional elements connected to an ESInet

---

[119] *Id.* at 8196, para. 132.
[120] *Id.* at 8180, para. 87; 47 CFR § 9.34.
[121] 47 CFR § 9.19(a)(4)(i)(A) (CSPs are entities that provide 911 call routing or location information "or the functional equivalent of those capabilities.").
[122] *911 Reliability Order*, 28 FCC Rcd at 17489, para. 37.
[123] NENA Comments at 2.
[124] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2684, para. 36.
[125] Appendix A (§ 9.19(a)(4)(i)(C), 9.19(a)(14), (15)).

that enable the real-time provision of 911 caller location information to PSAPs, including but not limited to the LVF, the ECRF, and successor technologies. We define NGCS routing facilities as functional elements connected to an ESInet that enable the real-time routing, delivery, or transfer of 911 traffic to PSAPs along with callback information and other associated data, including but not limited to the ESRP, the PRF, and successor technologies.[126] We emphasize that these listed NGCS elements are merely examples of transitional and future technologies performing routing and location functions, and are not intended to be exclusive.

We provide these clarifications because NG911 systems process routing and location information differently than legacy 911 systems. For example, the caller location function in NG911 does not rely on legacy ANI/ALI databases or MSAGs[127] to perform live-call location; instead, the LIS and LVF supply location data to other 911 functional elements through periodic updates typically.[128] As iCERT explains, while the LIS is functionally equivalent to legacy ALI/ANI databases and the LVF is functionally equivalent to the MSAG, the LVF may perform live-call critical functions in NG911 of validating location addresses as a 911 call is made.[129] As such, the prior rule does not perfectly correlate critical NG911 location and routing elements to their "functionally equivalent" legacy 911 service in every instance.[130]

We agree with commenters that suggest we include LVF and similar location validation functional elements as examples of covered NGCS functional elements, but only when used in live-call processing.[131] This modification addresses variation in how NGCS providers configure

---

[126] COPUC Comments at 3; Michigan State 911 Committee Comments at 1. *But see* NENA Comments at 5 (stating the PRF should be integrated with the ESRP and need not be listed). We include the PRF in light of the comment record reflecting variations in how NGCS systems are being deployed. *Compare* NENA Comments at 4, *with* iCERT Comments at 9 (disagreeing whether the LVF requires reliability in NGCS configurations); *compare* NENA Comments at 5-6, *with* iCERT Comments at 10 (disagreeing whether the MSAG Conversion Service, GeoCode Service, and Mapping Data Service functional elements require reliability in NGCS configurations).

[127] NENA, *NENA Knowledge Base,* https://kb.nena.org/wiki/MSAG_(Master_Street_Address_Guide), (last visited May 19, 2026).

[128] iCERT Comments at 10; NASNA Comments at 2.

[129] iCERT Comments at 10.

[130] APCO Comments at 8; NENA Comments at 1.

[131] *See*, *e.g.*, NASNA Comments at 2 (urging the exclusion of GIS as an NGCS Location Facility due to its "distance from the real time call flow" and acknowledging that an LVF can replicate legacy ALI/ANI real time location functionality); iCERT Comments at 9 (LVF "utilize[s] GIS information and data that are critical to the real-time routing and delivery of 911 calls within an NG911 environment"); Intrado Comments at 15 (Capabilities should not

the LVF to interface with other functional elements.[132] If an NGCS provider is using its location validation facilities for real-time location queries, those facilities are subject to our 911 reliability framework. If a NGCS provider has chosen to arrange its system so that its location validation facilities only periodically send information to a LIS or other NGCS element, then the LVF is being used more like the GIS, and thus there is no need to include it as a covered 911 facility.

In addition to the LVF, we include the ECRF as an example of covered live-call NGCS location facilities, and the ESRP and the PRF as examples of covered live-call NGCS routing facilities. While we provide these specific examples, we also retain the "functional equivalent" language from the prior rule to capture both transitional NG911 elements and future technologies that may be developed to perform NGCS functions. As NASNA notes, including transitional routing and location functional elements as covered 911 facilities is important to ensure transitional 911 systems remain reliable.[133] For example, IP selective routers and IP ALI databases are examples of transitional architecture that may perform basic IP routing and location functions at an ESInet before a 911 Authority has built and deployed full NGCS routing and location capabilities.[134]

Some commenters question whether certain NGCS elements—such as MSAG Conversion Service, GeoCode Service, and Mapping Data Service—are needed for 911 live-call routing or location information.[135] The functional definition we adopt today resolves the issue by including these functions only when the NGCS provider uses them for live-call routing or location information. We also agree with NENA and other commenters that recommend against

---

be covered if they are "outside the call flow and [are] not directly related to real-time call routing or transmission of caller location information.").

[132] NENA Comments at 4; iCERT Comments at 9.

[133] NASNA Comments at 1 (noting the importance of protecting reliability during the NG911 transition).

[134] NENA NG9-1-1 Transition Plan, Considerations Information Document, at 56 (Nov. 20, 2013) https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/standards1/NENA-INF-008.2_NG9-1-1Transi.pdf ("[A]n Internet Protocol Selective Router (IPSR) function . . . is an IP-based Selective Router that that provides E9-1-1 functionality while incorporating the ability to receive native SIP emergency calls" and deliver them to PSAPs); *see also* Indiana Statewide 911 Board, The History of Accomplishments of 911 in Indiana, at 17 (Nov. 2020) https://www.in911.net/uploads/1/2/4/9/124957688/2020_history_and_accomplishments_final.pdf ("INdigital customers receive ALI via a distributed IP ALI system (INDB). This will change with the full deployment of the dual ESInets.").

[135] NENA Comments at 5-6; iCERT Comments at 10.

including GIS as an example of covered NGCS Location Facilities. GIS is a "a system for capturing, storing, displaying, analyzing, and managing data and associated attributes which are spatially referenced" to map and visualize data such as the locations of streets and buildings.[136] While GIS plays an important role in NG911, we exclude it because it is not used for the delivery of real-time 911 caller location information. Instead, GIS is a data resource that supplies information to a LIS or NGCS element only periodically so that those covered elements can perform the live caller location function.[137]

Direct Service to 911 Authorities. As proposed in the *NG911 Reliability FNPRM*, we require providers of NGCS covered 911 services to comply with the 911 reliability framework when providing such services directly, by contract or tariff, to a 911 Authority, whether via owned and operated facilities or leased or contracted facilities.[138] While some commenters support extending reliability requirements for NGCS functional elements to services provided indirectly as well as directly to 911 Authorities, we are persuaded by commenters who argue that the Commission should avoid adopting overbroad regulations that could increase 911 Authorities' and PSAPs' costs.[139] We agree with NASNA that CSP obligations should fall on the NGCS "primary provider" in a jurisdiction, instead of on every NGCS subcontractor.[140] We also agree with APCO and other commenters that direct regulation of NGCS subcontractors is excessive and unnecessary, because the CSP providing direct service is best positioned to ensure reliability and because direct regulation of a CSP's third-party contractors could unnecessarily increase costs.[141] We therefore decline to follow the suggestion of NENA and other commenters asking to directly cover any NGCS routing and location service subcontractor regardless of its

---

[136] NENA, *NENA Knowledge Base*, https://kb.nena.org/wiki/GIS_(Geographic_Information_System) (last visited May 19, 2026); *see also NG911 Transition Order*, 39 FCC Rcd at 8224-25, para. 191 & n.566.
[137] NASNA Comments at 2; NENA Reply at 2; DATAMARK Technologies (DATAMARK) Reply at 4-5.
[138] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2684-85, paras. 36, 39.
[139] City of Coconut Creek, FL July 21, 2025 Comments at 1.
[140] NASNA Comments at 2 ("The FNPRM delves into the complexities of layers within the NG911 ecosystem and contractual/sub contractual relations, and the rules need to be clear that the responsibility for the 911 jurisdiction's network reliability lies within the primary provider as defined and set forth by the 911 jurisdiction.").
[141] APCO Comments at 7; Texas 9-1-1 Entities Comments at 3; Intrado Comments at 14; T-Mobile Comments at 2; NCTA Reply at 4-5.

relationship to 911 Authorities.[142] However, as discussed in more detail below, we apply the 911 reliability framework independently to a narrow subset of critical NG911 facilities (ESInets and associated transitional gateways) that may be provided by the NGCS provider or its subcontractors.

Finally, as recommended by several commenters, we replace the word "PSAP" with "911 Authority" to ensure all necessary NGCS entities are covered. This change is necessary to account for the variety of state and local governance structures for 911,[143] and we incorporate the definition of "911 Authority" adopted in the *NG911 Transition Order*.[144]

Administrative Lines. Some commenters advocate revisions to remove administrative lines from the definition of essential facilities to be maintained by legacy CSPs.[145] We decline to revise the legacy 911 reliability definition at this time, because TDM-based administrative lines continue to be used in legacy PSAPs as a backup option during outages as well as for PSAP-to-PSAP calls.[146] However, we anticipate that this requirement will become moot as legacy PSAPs replace TDM administrative lines with VoIP connectivity delivered by ESInets.[147] Accordingly, we encourage 911 Authorities, PSAPs, CSPs, and OSPs to work together to quickly migrate and retire legacy TDM facilities consistent with the overall goals of the NG911 transition and the IP transition. As the NG911 transition progresses, the Commission may re-evaluate the continued importance of reliability requirements for legacy administrative lines.

---

[142] NENA Comments at 3; CCOA Comments at 2-3; Comtech Comments at 14-15. *See also* Michigan State 911 Committee Comments at 1 (encouraging the Commission to hold indirect providers accountable "either through direct certification or through clear responsibility by the contracting [CSP]").

[143] NENA Comments at 3; Brian Rosen Reply at 2.

[144] *NG911 Transition Order*, 39 FCC Rcd at 8164, para. 50; 47 CFR § 9.28.

[145] NASNA Comments at 3; *see also* NCTA Reply at 6 & n.20. The term "legacy CSP", when used in this *Order*, refers to providers of TDM-based 911 or E911 covered services under the original 2013 reliability rules. *See* 47 CFR § 9.19(a)(4)(i)(A)-(B).

[146] *See 2020 Best Practices Public Notice*, 35 FCC Rcd at 13179-81 ("If primary and secondary routing to . . . [PSAPs] are not available, [CSPs] and [OSPs] should take steps to ensure that the 911 caller receives assistance, such as routing 911 calls to the administrative lines of destination PSAP(s)[.]").

[147] NC 911 Board, North Carolina 911 Board Meeting Minutes for Aug. 28, 2020 at 7 (2020), https://it.nc.gov/20200828-nc911-board-minutes-approved/download?attachment (discussing the "conversion of PSAP administrative lines to SIP to provide additional capabilities and protection" and stating that doing so "would also provide cost savings in the long run. Not all administrative lines could be converted . . . and this could only be done for those utilizing a hosted call handling solution on the ESInet.").

ESInets and Legacy PSAP Gateways

As proposed in the *NG911 Reliability FNPRM*, we designate the operation of ESInets, as covered 911 services subject to our 911 reliability framework.[148] The Commission has historically treated ESInet providers as CSPs to the extent they provide covered 911 services.[149] The Commission has also recognized that ESInet paths to PSAPs are "critical 911 circuits" under the 2013 rules.[150] The *NG911 Reliability FNPRM* proposed to explicitly identify ESInet transport paths to PSAPs as covered facilities.[151] We adopt this proposal in today's *Order*, affirming that operation of an ESInet is a covered 911 service. This recognizes the fact that ESInet operators typically manage critical NG911 circuits and paths needed to receive and process 911 calls from OSPs and transmit them to 911 telecommunicators, forming the "backbone" of NG911.[152] As a practical matter, identifying ESInet operators as CSPs is not a major rule change, because most current ESInet operators have already filed 911 reliability certifications under the prior rules.

Because of the central and critical role of transport performed by ESInets in the NG911 ecosystem, we classify all ESInet providers as CSPs regardless of whether they provide services directly or indirectly to a 911 Authority. As NENA notes, there may be instances where a regulation covering NGCS providers "directly serving" a 911 Authority may not capture corresponding ESInet providers, as the two entities might be separate with only one of the two having a contract with the 911 Authority.[153] To accommodate potential variation in state and local government NG911 deployments and ensure that all ESInets meet reliability standards, we

---

[148] Appendix A (§ 9.19(a)(4)(i)(D)).
[149] *911 Reliability Order*, 28 FCC Rcd at 17491, para. 43 ("[W]e decline at this time to cover all operators of [ESInets][.] . . . ESInet operators will be required to certify reliability only to the extent they qualify as Covered 911 Service Providers under our rules.").
[150] *Id*. at 17503, para. 81 & n.179 ("NG911 networks may use IP-based ESInets to interconnect the selective router function to the PSAP. The facilities that compose these ESInets would be considered 'critical 911 circuits.'").
[151] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2694, para. 65 (NG911 data paths subject to physical diversity "include[] IP traffic paths from NGCS facility capabilities . . . ."); *id.* at 2689, para. 53 (asking if the proposed rules would "capture instances where ESInet operators accept 911 traffic at an NG911 Delivery Point, send the traffic out of state for processing, and then back in-state to the ESInet for ultimate delivery to a PSAP").
[152] NENA, *NENA Knowledge Base*, https://kb.nena.org/wiki/ESInet_(Emergency_Services_IP_Network) (last visited May 19, 2026).
[153] NENA Comments at 12.

include the operation of an ESInet as a covered 911 service whether the service is provided directly or indirectly to 911 Authorities.

Transitional Legacy PSAP Gateways. We also include NG911 transitional gateways used with ESInets as covered 911 services.[154] Specifically, we include legacy PSAP gateways (LPGs) as covered transitional elements, which link NGCS and ESInet facilities to legacy PSAPs, permitting 911 Authorities to upgrade PSAPs to NG911 on a graduated basis as funding and resources become available.[155] As with all of the CSP categories we adopt today, if an LPG is operated directly by the PSAP or 911 Authority instead of a private vendor, it is excluded from our covered 911 services definition and no certification is required.

Other services. Some commenters claim they lack visibility into the network path diversity of their downstream or leased transport providers and therefore cannot implement 911 reliability measures with respect to those facilities.[156] Some of these commenters ask the Commission to directly regulate the ESInets' underlying transport providers or Multiprotocol Label Switching (MPLS) vendors as CSPs.[157] While we decline to classify such underlying transport or MPLS providers as CSPs independently, we agree that ESInet providers should not be required to certify to the network architecture of IP paths beyond the information they can reasonably obtain in service level agreements.[158] Accordingly, and as discussed further below, we adopt additional safeguards and certification processes to ensure that all CSPs, including ESInet operators, can certify to the Commission that they satisfy reasonable reliability based on measures that they themselves can implement.

---

[154] Appendix A (§ 9.19(a)(4)(i)(F)).
[155] *See* Mike Guerra, Director of NG9-1-1 Products, AT&T, *Keeping 9-1-1 Connected as Networks Evolve: How T9-1-1 Bridges the Gap for PSAPs* (Jan. 20, 2026), https://about.att.com/blogs/2026/t911.html (describing a solution with which AT&T will use legacy PSAP gateways to maintain connectivity with legacy PSAPs during the IP transition).
[156] Comtech Comments at 14-15; Intrado Comments at 20; iCERT Comments at 13.
[157] Comtech Comments at 15; NENA Comments at 9. *See also* NENA, NENA Knowledge Base, https://kb.nena.org/wiki/MPLS_(Multiprotocol_Label_Switching) (last visited May 19, 2026) (defining MPLS).
[158] iCERT Comments at 13.

Location Information Servers and Transitional Gateways

In the *NG911 Reliability FNPRM*, the Commission proposed to include Location Information Servers (LISs) and Legacy Network Gateways (LNGs) in the definition of covered 911 services because these services are critical to the call path of 911 traffic.[159] A LIS is an NG911 functional element that allows OSPs to send caller location information to PSAPs for IP networks, replacing the legacy ALI/ANI database.[160] An LNG converts TDM 911 traffic from OSPs to IP format before it reaches an NG911 ESInet, and as such it is critical to ensure 911 reliability during the NG911 transition.[161] Unlike LISs, LNGs are transitional facilities that will be phased out when the NG911 transition is complete.

We adopt the *FNPRM* proposal to include LISs and LNGs in the definition of covered 911 services, but only for operators that provide LIS or LNG services to two or more OSPs.[162] This modification addresses concerns raised by wireless industry commenters that operate LIS and LNG facilities for their own traffic only.[163] We clarify that the 911 reliability framework does not apply to OSPs that self-provision a LIS or LNG, to OSPs that contract with providers of aggregated LIS or LNG services, or to LIS/LNG providers that only serve a single OSP.[164]

To provide additional clarity as to the 911 services addressed in our 911 reliability framework, we also include operators of emergency services gateways (ESGWs), which provide critical connectivity between IP paths and legacy trunks connecting to a selective router, and operators of legacy selective router gateways (LSRGs), which provide an interface between legacy selective routers and ESInets during the transition until IP facilities are installed to replace all TDM facilities in the 911 call path between the OSP and the ESInet.[165] Similarly to the LNG

---

[159] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2686-87, paras. 44-46.
[160] *NG911 Transition Order*, 39 FCC Rcd at 8170-71, para. 70; *see also* 47 CFR § 9.28 (defining "LIS").
[161] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2687, paras. 45-46.
[162] Appendix A (§ 9.19(a)(4)(i)(E)-(F)).
[163] *See*, *e.g.*, CTIA Comments at 3-4.
[164] NCTA Reply at 6; Letter from Steven Morris, Vice President and Deputy General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 21-479 *et al*., at 2 (filed May 4, 2026) (NCTA May 4, 2026 *Ex Parte*).
[165] *CSRIC VI WG 1 Report* at 129 ("The LSRG provides an interface between a 9-1-1 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1."); NENA, NENA Legacy Selective Router Gateway (LSRG) Standard at 2 (2022), https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-034.1-2022_lsrg_202.pdf. *See*

and LIS, we limit coverage of transitional gateways on the OSP side of the call path to those that serve two or more OSPs. Therefore, OSPs that self-provision their own transitional gateways without offering service to other OSPs, while subject to the OSP 911 transmission rules, are not subject to the 911 reliability framework.

We disagree with commenters who argue against including shared LIS and LNG facilities as covered 911 services, as they are unambiguous chokepoints in NG911 architecture, not subject to state and local governmental or Commission direct visibility and oversight under the 2013 reliability rules, and can benefit from reasonable reliability measures. At the same time, we agree with commenters that it is not necessary to apply the full array of reliability obligations to LIS and LNG facilities that apply to other critical NG911 elements. Therefore, we are not imposing automatic rerouting or load balancing obligations on LIS, LNG, or similar transitional covered 911 facilities—which are IP path reliability standards—but only the operational integrity benchmarks which apply to server facilities and similar equipment. We also acknowledge that the LNG is a mixed TDM-IP transitional network element that may not always be able to provide automatic switchover to redundant facilities depending on behaviors of the "sending carrier's" facilities.[166] We reiterate that CSPs may certify to the Commission that they are using alternative reliability measures based on technology or customer limitations. In addition, as will be the case with similar transitional mixed TDM-IP facilities like the LPG, we will not dictate to CSPs whether their LNGs, LSRGs, or ESGWs should satisfy IP reliability practices or legacy reliability practices; so long as they satisfy one or the other, we will deem the practices presumptively reasonable. We defer to CSPs to implement the most reasonable combination of practices under the circumstances, including practices that pick and choose from both categories as alternative measures.

Finally, we agree with Intrado that "the aim should be to eliminate these LNGs as quickly

---

also NENA, NENA Knowledge Base, ESGW (Emergency Services Gateway), https://kb.nena.org/wiki/ESGW_(Emergency_Services_Gateway) (last visited May 30, 2026).

[166] Intrado Comments at 18.

as possible by accelerating end-to-end NG911."[167] The Commission is actively engaged in multiple proceedings to expedite the NG911 and IP transitions.[168] We take this opportunity to encourage all CSPs, OSPs, and 911 Authorities to continue to work expeditiously and cooperatively to retire their legacy TDM-based facilities to upgrade and replace them with IP and NG911 facilities as fast as possible. The NG911 and IP transitions are interdependent and necessitate stakeholders in the NG911 ecosystem to coordinate, including around ensuring the reliability of 911 for the benefit of consumers. Today's 911 reliability framework will provide greater visibility into how the NG911 transition is working for state and local governments and for the Commission and will allow us to exercise better oversight into these transition processes, and to help resolve problems where they arise.

Major IP Transport Facilities and IP 911 Traffic Aggregation Facilities

We categorize providers of both major IP transport facilities and 911 IP aggregation facilities as CSPs, consistent with the Commission's proposals in the *NG911 Reliability FNPRM*.[169] However, in response to the record, we have narrowed the scope of our definitions of major IP transport facilities and 911 IP traffic aggregation facilities to focus on large-scale transport and aggregation facilities that would have the most significant impact on 911 service in the event of an outage. For major IP transport facilities, we raise the capacity threshold of services that would be subject to the 911 reliability framework. Moreover, for both major IP transport and 911 IP aggregation, we include such providers within our definitions only if they provide services to two or more OSPs, excluding any 911 traffic originated on the provider's own network.

In legacy 911, most OSPs deliver 911 calls directly to their local ILEC, which uses selective routers to receive and route the calls to the appropriate PSAP. When the Commission

---

[167] *Id.*

[168] *See*, *e.g.*, *NG911 Transition Order*, 39 FCC Rcd at 8137, para. 1; *Advancing IP Interconnection et al*., WC Docket No. 25-304 et al., Notice of Proposed Rulemaking, FCC 25-73, 2025 WL 3677909 (Oct. 29, 2025); *Reforming Legacy Rules for an All-IP Future; Accelerating Network Modernization*, WC Docket Nos. 25-311 and 25-208, Notice of Proposed Rulemaking, FCC 26-11, 2026 WL 567517 (Feb. 19, 2026).

[169] Appendix A (§ 9.19(a)(4)(i)(G)-(H)); *NG911 Reliability FNPRM,* 40 FCC Rcd at 2687-89, paras. 47-53.

identified selective routers as critical 911 facilities in the 2013 *911 Reliability Order*, it recognized that selective routers perform not only the routing function but also aggregate 911 calls from multiple OSPs.[170] In the *NG911 Reliability FNPRM*, the Commission recognized that, in NG911 architecture, the routing and aggregation functions previously performed by ILEC selective routers are performed by an entirely new set of routing and aggregation facilities. Moreover, many of these routing and aggregation facilities are provided by third parties who operate downstream from OSPs but upstream from the POIs where 911 traffic is handed off to ESInets for routing to the appropriate PSAP.[171] In the *FNPRM*, the Commission noted that these facilities were not subject to the Commission's 911 transmission rules or the then-current 911 reliability rules because providers of third-party transport and aggregation services did not meet the definition of either CSPs or OSPs.[172] The Commission tentatively concluded that these providers had become sufficiently crucial to the provision of NG911 service that they should be subject to the same reliability requirements as other providers of covered 911 services.[173] The Commission also proposed to focus reliability requirements on major transport and aggregation providers and not to extend them to smaller providers whose facilities do not pose a risk of widespread 911 outages.[174]

Public safety commenters emphasize the importance of including third-party transport and aggregation services in the definition of covered 911 services.[175] These commenters also confirm that several recent significant 911 outages have resulted from failure of these facilities.[176] To date, neither the Commission nor 911 Authorities have had sufficient visibility into or oversight of these critical NG911 market participants to ensure reliable 911 services.[177]

---

[170] *NG911 Reliability FNPRM* at 2694, para. 65 & n.141 (citing *911 Reliability Order*, 28 Rcd at 17478, para. 7 ("The local switch then sends the call to an *aggregation point* called a selective router[.]")).
[171] *Id*. at 2677, para. 17.
[172] *Id.* At 2687-88, para. 48.
[173] *Id*. at 2687, para. 47.
[174] *Id*. at 2688, para. 49.
[175] NYPSC Comments at 2; CCOA Comments at 2; NENA Comments at 1-2.
[176] NENA Comments at 1-2; COPUC Comments at 2.
[177] Brian Rosen Reply at 2; CCOA Comments at 2.

Designating the operators of these facilities as CSPs will ensure that the reliability practices of these critical providers in the 911 call path are visible to 911 Authorities and the Commission in the event that problems or call failures arise.[178]

Our action also provides greater certainty for OSPs contracting with third-party CSPs to provide 911 transport or aggregation. OSPs express concern that they could face increased risk of liability for 911 outages caused by failures of third-party NG911 transport providers and aggregators if such entities are not subject to FCC regulation and oversight.[179] Today's 911 reliability framework extending FCC oversight to transport providers will allow OSPs to better vet their NG911 third-party CSPs based on the FCC's NG911 reliability benchmarks. Similarly, strengthening the reliability of third-party aggregation services benefits OSPs by providing additional assurances that entities responsible for aggregating their customers' 911 calls are taking measures to support reliability.[180]

We disagree with commenters who contend that the 911 transmission rules applicable to OSPs are sufficient to ensure reliability of third-party 911 transport and aggregation between OSPs and ESInets.[181] While the 911 transmission rules, in conjunction with the NG911 transition framework, hold OSPs responsible for delivering 911 calls originated on their networks to ESInets and PSAPs, they do not impose any specific reliability obligations on the third parties that many OSPs rely on to accomplish such delivery. Moreover, as the Commission recognized in the *NG911 Reliability FNPRM*, the reliability practices of these third parties may be invisible to OSPs until after an outage has occurred.[182] By applying the 911 reliability framework to third-party providers, we enable 911 Authorities and the Commission to work

---

[178] NYSPSC Comments at 1-2; COPUC Comments at 7.
[179] Home Telephone NG911 Transition Comments, PS Docket 21-479, at 5 (rec. Aug. 9, 2023) ("[S]everal large Aggregators will be consolidating massive portions of the country's critical emerging NG911 services on their systems with little Commission oversight."); *id*. at 13 & n.6, 16-17; Windstream NG911 Transition Reply, PS Docket 21-479, at 2-3 (rec. Sep. 8, 2023).
[180] Home Telephone NG911 Transition Comments, PS Docket 21-479, at iii (rec. Aug. 9, 2023) ("The Commission should establish standards and reporting requirements for these 'Aggregators' to ensure the NG911 network is safe and reliable for IP emergency transmissions destined to local PSAPs."); Windstream NG911 Transition Reply, PS Docket 21-479, at 2-3 (rec. Sep. 8, 2023).
[181] Verizon Comments at 6-7; CTIA Comments at 4; USTelecom Reply at 2-3.
[182] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2677, para. 18.

collaboratively with industry and state and local governments to *prevent* these kinds of 911 outages before they happen.[183] The Commission's goal, through the application of this 911 reliability framework to major IP transport and IP 911 traffic aggregation facilities, is to reduce the risk of multistate or multi-OSP 911 outages such that there are fewer instances in which callers cannot reach their local PSAP in case of emergency.

We also disagree with commenters who contend that extending our 911 reliability framework to third-party providers will result in OSPs necessarily bearing unwarranted additional costs for NG911 reliability.[184] Under the NG911 transition framework, OSPs are presumptively responsible for the costs of 911 transport to NG911 delivery points, whether they provide such transport directly or through a third-party provider. However, requiring third-party providers to take reliability measures gives OSPs more options, not fewer, for controlling such costs while reducing their outage risk.[185] OSPs retain flexibility to use dedicated third-party CSP transport or aggregation services or to directly connect to ESInets. OSPs that choose to use third-party CSPs will have greater assurance that the CSPs are providing reliable dedicated service. OSPs also have cost-effective options to purchase geo-diverse cloud-based paths or VPN circuits over the public Internet—neither of which is itself a covered 911 service, but both of which, with suitable precautions, can help OSPs or CSPs to achieve 911 path diversity and ensure reliable 911 traffic delivery. OSPs may also reduce costs by reaching agreements to use the same IP paths between ESInets and PSAPs to send originating customer 911 traffic upstream to reach the NGCS facilities.[186]

Major IP transport facilities. In the *NG911 Reliability FNPRM*, the Commission proposed

---

[183] NYSPSC Comments at 2; Virginia State Corporation Commission Comments, PS Docket No. 13-75 et al., at 4 (rec. Mar. 23, 2015) ("[I]n the public safety arena the priority must be on prevention versus determining blame after a tragic event.").
[184] NTCA and the RLEC Parties Comments at 2, 4-5.
[185] *Id*. at 4-5.
[186] Home Telephone Comments at 10-11 & n.32 ("The concept would utilize the connection between the ESInet provider and the PSAP which is used to transmit information down to the PSAP on a two-way basis to transmit traffic from the OSP back to the ESInet. . . . Thus, the need for new or separate facilities for the transmission from the OSP to the ESInet is eliminated, reducing cost, complexity, and potential failure points.").

to apply reliability requirements to major transport facilities providers, defined as providers offering OC3 or higher capacity (155 Mbps), and to exclude smaller transport providers with capacity below this threshold. Some commenters argue that the proposed threshold for major IP transport is too low and could be costly when applied to rural areas, or even impossible to achieve in some cases.[187] We agree with these commenters that compliance with the reliability requirements imposes some costs, and that IP transport providers serving small and rural areas may face a greater cost burden. To address these concerns, we are raising the threshold for IP major transport to focus on the largest transport facilities that pose the greatest risk of causing multistate or multi-OSP 911 outages.[188]

We define major IP transport facilities as dedicated SIP voice and text transport facilities meeting or exceeding Optical Carrier 48 (OC48) / 2.5 Gbps in capacity that collect and/or transmit IP 911 traffic mixed with non-911 traffic from two or more OSPs, and transport it over interstate dedicated SIP routes, for ultimate delivery to an NG911 Delivery Point or equivalent ESInet point of interconnection. The threshold for major IP transport facilities includes any 2.5 Gbps equivalent or higher capacity transport facilities, whether using OC, ethernet, or another technology. We clarify that this CSP definition of major IP transport capacity does not alter any existing Network Outage Reporting System obligations under part 4 of our rules.[189]

Consistent with the *NG911 Reliability FNPRM* proposals and goals, we differentiate between major IP transport providers, which we designate as CSPs, and general Internet transit providers, which we do not designate as CSPs.[190] Major IP transport providers are those network

---

[187] Lumen Comments at 4-5; Verizon Comments at 13-14; Verizon Reply at 4 & n.12.
[188] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2689, para. 53 (asking if the OC capacity threshold should be updated with a Gbps equivalent).
[189] *See* 47 CFR § 4.7(d) (defining OC3 user minutes for determining NORS outage reporting threshold criteria). Under the NORS reporting requirements, cable communications providers, IXC or LEC tandem facilities providers, satellite operators, SS7 providers, wireless service providers, and wireline communications providers must submit electronically a notification to the Commission when the outage threshold criteria pertaining to each service have been met. *See* 47 CFR § 4.9(a)-(g). While an entity defined as a CSP may be required to report in NORS, it would be by virtue of its status as one of the entities regulated under § 4.9(a)-(g) and not because of its status as a CSP.
[190] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2688, para. 49 ("[W]e propose to limit the definition Major Transport Facilities to providers that operate dedicated SIP transport facilities . . . ."); *id.* at 2695, para. 66 ("We note that today's proposed rules are not meant to capture every single transit provider of general Internet traffic, but rather

operators that meet the OC48/2.5 Gbps threshold and offer dedicated SIP service that includes voice and/or text to two or more OSPs for 911 traffic. General Internet transit includes public Internet, VPN, or cloud-based service products and their underlying transport networks that provide IP connectivity but do not offer dedicated voice or text service.[191] For the reasons NENA explains, we anticipate that OSPs, CSP major IP transport providers, and other CSPs may use general Internet paths as diverse pathways for transport of 911 traffic to ensure 911 reliability.[192] We seek to encourage and not to foreclose use of these available paths to support diversity and redundancy in the NG911 ecosystem.[193] Therefore, while we apply our 911 reliability framework to CSPs even if they choose to use general Internet transit paths for redundancy or downstream transmission, we do not classify the Internet transit providers or their underlying transport networks as CSPs, and we exclude them from the CSP regulatory framework. Such regulation is unnecessary and would be highly burdensome; in addition, no commenter has requested regulation of Internet paths.

We provide relief to some OSPs offering IP transport facilities that otherwise meet the OC48/2.5 Gbps threshold by further limiting the definition of major IP transport facilities to those transporting the 911 traffic of two or more OSPs. To account for instances in which a major IP transport facility provides transport to another OSP on an incidental basis, we exclude 911 traffic originated on the provider's network in the determination of whether a particular facility is transporting the 911 traffic of two or more OSPs. Accordingly, an OSP that transports its own voice and text 911 traffic, plus the 911 traffic of one other OSP, is not a provider of major IP transport facilities, regardless of whether it meets the increased threshold definition. We agree with NCTA that this change helps us achieve our goals of balanced regulation by requiring reliability best practices only for network facilities carrying substantial risk of multi-

---

dedicated transport providers that carry *substantial* 911 traffic.") (italics added); *id.* at 2729, Appendix A, Proposed Rule 9.19(a)(12) (defining "Major Transport" as "Dedicated SIP transport facilities").

[191] NENA Comments at 10-11.

[192] *Id*.

[193] *Id*.

OSP outages.[194] This change also avoids imposing undue burdens on OSPs that provide limited and incidental third-party transport services.[195] To harmonize our 911 reliability framework and ensure consistency, we apply these same changes to the definition of IP 911 traffic aggregation facilities, which must carry 911 traffic for two or more OSPs, not counting any 911 traffic originated on the facility provider's own network.

We further exclude any dedicated SIP transport that is exclusively used to carry data traffic with no dedicated OSP voice or text to avoid capturing non-911 transport, as requested by NCTA and Intrado.[196] We believe these exclusions narrow the proposal sufficiently to avoid unnecessary burdens.[197] Accordingly, our definition of major IP transport facilities includes providers that comingle 911 traffic transport from two or more OSPs with general OSP voice traffic. We believe this revised definition reasonably ensures reliability of major NG911 traffic conduits to ESInets without overburdening industry. Our priority is the reliability of the largest interstate transport routes and facilities carrying 911 traffic from two or more OSPs, the failure of which poses the greatest risk to the transmission of 911 traffic for the public. Today's modifications accomplish this goal, while also creating regulatory certainty for business and avoiding undue burdens and costs for entities that provide IP transport but carry little or no dedicated 911 traffic.

Our implementation of these exclusions, and raising of the IP transport capacity threshold, mitigate concerns raised by commenters that some IP transport providers may be unable to ascertain whether they carry 911 traffic.[198] Because only large providers that serve two or more OSPs fall under the major IP transport definition, we believe it is reasonable to expect them to inquire as to whether or infer that they carry 911 traffic. Under the Commission's robocall mitigation and know-your-customer rules, voice service providers have an affirmative

---

[194] NCTA May 20, 2026 *Ex Parte* at 3.
[195] *Id.*
[196] NCTA Reply at 7 (quoting Intrado Comments at 18).
[197] NCTA May 4, 2026 *Ex Parte* at 2.
[198] Verizon Comments at 7-8; Lumen Comments at 6-8.

responsibility to know their upstream providers and the nature of the traffic they are receiving from those providers to ensure their networks or services are not being used to transmit illegal calls.[199] The Commission's call blocking rules also require or permit providers to block calls under certain conditions, but place robust restrictions on blocking of 911 and other emergency calls.[200] At most, the downstream providers of high-capacity, interstate long-haul dedicated SIP transport must ask OSPs or upstream providers whether their traffic includes 911 traffic, or if the OSP has segregated out its 911 traffic prior to handoff. To the extent major IP transport providers are not already inquiring about this from their upstream customers, we believe it is a reasonable measure to reduce the risk of large-scale 911 outages.

IP 911 traffic aggregation facilities. The Commission proposed in the *NG911 Reliability FNPRM* to require third-party operators of IP-based 911 aggregation facilities to implement reliability practices because a large percentage of 911 traffic passes through such facilities.[201] The Commission stated in the *FNPRM* that IP 911 aggregation facilities have become critical to the transmission of 911 traffic,[202] and that IP 911 aggregation services have already emerged as a

---

[199] *See* 47 CFR § 64.1200(n)(5) (requiring that all voice service providers "[t]ake reasonable and effective steps to ensure that any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using the provider to carry or process a high volume of illegal traffic onto the U.S. network"); *see also Lingo Telecom, LLC*, File No. EB-TCD-24-00036425, Consent Decree, 39 FCC Rcd 9304, 9316-17, paras. 3-4 (EB 2024) (requiring specific know-your-upstream-provider compliance requirements for "any customer who purchases a SIP Trunking Product from Lingo Telecom" and "prior to transmitting any call as a gateway or intermediary provider on behalf of any immediate upstream provider"). The Commission recently proposed further strengthening the know-your-upstream provider rules. *Call Authentication Trust Anchor, Advanced Methods to Target and Eliminate Unlawful Robocalls*, WC Docket No. 17-97, CG Docket No. 17-59, Further Notice of Proposed Rulemaking, FCC 26-32, at 8-18, paras. 14-28, 2026 WL 1284762, at *5-8 (May 21, 2026) (proposing to strengthen the know-your-upstream-provider rule and require that voice service providers follow specific measures to fulfill their obligations under that rule).

[200] *See* 47 CFR § 64.1200(k), (n), (o) (describing required and permissive call blocking practices); *id.* at 64.1200(k)(5)-(6) (requiring providers that block calls consistent with the Commission's rules make all reasonable efforts to avoid blocking calls from PSAPs and government outbound emergency numbers and never block emergency calls to 911 unless the provider knows without a doubt that the calls are unlawful); 47 CFR § 64.6305(g) (prohibiting providers from accepting calls directly from a domestic voice service provider that does not appear in the Robocall Mitigation Database); *id*. at 64.6305(g)(5) (providing that, notwithstanding that prohibition, "[a] provider may not block a voice call under any circumstances if the call is an emergency call placed to 911; and (ii) [a] provider must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers").

[201] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2688, para. 50.

[202] *Id.* at 2687-89, paras. 47-53.

significant market during the transition to NG911.[203] The record confirms that IP 911 traffic aggregation is a critical NG911 function that should be covered by our 911 reliability framework.[204] We therefore designate IP-based 911 aggregators as CSPs to ensure visibility and oversight into providers for which OSPs may not have substantial leverage or practical control, and for which the FCC and state and local governments lack visibility or oversight.

We define IP 911 traffic aggregation facilities as IP-based facilities that collect and segregate 911 traffic from non-911 traffic for two or more OSPs, or that aggregate and transport 911-only traffic from two or more OSPs for ultimate delivery to NG911 delivery points.[205] Unlike major IP transport facilities, for which we define a capacity threshold, we do not put such a threshold on IP-based 911 aggregation facilities because, by definition, these facilities handle only 911 traffic. Any entity that collects and segregates IP 911 traffic from non-IP 911 traffic on behalf of two or more OSPs must meet the reliability requirements because the aggregation of 911 traffic creates a heightened risk to 911 callers if there is an outage. We reiterate that an OSP hiring an IP 911 traffic aggregator is not a CSP, nor is an OSP providing 911 IP aggregation for its own traffic or that of its wholly-owned subsidiaries or operating companies.[206] We also include reference to "911" in the name of this CSP category to avoid confusion with more general IP traffic aggregation facilities not collecting 911-only traffic.[207]

IP 911 traffic aggregators that lack visibility into the paths of their 911 traffic via underlying networks may certify to the reliability measures they are taking in the same way we have specified for ESInet operators.[208] Specifically, IP 911 traffic aggregators may identify the underlying network providers they have retained to ensure path diversity, the visibility into

---

[203] Lumen Comments at 1 (stating that Lumen is a transport provider and an aggregator of 911 IP traffic in several states); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2688, 2692, paras. 50, 60 & nn.105-106, 129 (describing 911 IP aggregation services of Sinch and Bandwidth).
[204] NYPSC Comments at 2; CCOA Comments at 2.
[205] As with major IP transport facilities, we define "two or more OSPs" for IP 911 traffic aggregation to exclude 911 traffic originating on the provider's own network.
[206] NCTA May 4, 2026 *Ex Parte* at 2.
[207] NCTA Reply at 8-9.
[208] Intrado Comments at 18; Verizon Comments at 9.

network architecture those providers offer via service level agreements, and any additional multi-homing, cloud-based, or VPN backup measures the IP 911 aggregator is using to ensure path diversity. As in the case of underlying network providers that support ESInet operations, underlying network providers that contract to carry the traffic of a 911 IP aggregator are not CSPs if they do not otherwise meet the CSP definition.[209] However, we recognize that market arrangements are not identical across the NG911 ecosystem, and we want to ensure our 911 reliability framework is flexible enough to adapt to changing conditions. Accordingly, in situations where OSPs segregate 911 traffic on their own network and send it to a third-party carrier for dedicated SIP transport, those third-party carriers would also be CSPs under the IP 911 traffic aggregator definition we adopt, provided they aggregate 911 traffic from two or more OSPs.[210] We reiterate that, in such cases, the same minor effort we expect of major IP transport providers to inquire of their customers or upstream providers would apply to IP 911 traffic aggregators as well.[211]

Interstate Interconnecting ESInet Facilities

We adopt the proposal from the *NG911 Reliability FNPRM* to designate operators of interstate interconnecting facilities between ESInets as covered 911 service providers.[212] Interstate interconnecting ESInet facilities are interstate facilities that transport IP 911 traffic from an ESInet for ultimate delivery to another ESInet, including facilities designated for intermittent, contingent, or backup exchange of IP 911 traffic between ESInets. We believe it is reasonable to treat interstate ESInet interconnection providers as CSPs in instances where 911 Authorities elect to connect ESInets with one another across state lines. Connections between ESInets can provide important resiliency during natural disasters and other major emergencies,[213]

---

[209] Verizon Comments at 8-9.
[210] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2695, para. 66 (seeking comment on ensuring the class of 911 IP aggregator CSPs subject to path diversity benchmarks captures enough critical facilities).
[211] *Cf.* Verizon Comments at 8-9 (arguing IP 911 aggregators might not have visibility into their OSP customers' traffic).
[212] Appendix A (§ 9.19(a)(4)(i)(I)); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2689-90, paras. 54-55.
[213] NENA Comments at 8.

but only if those connections between ESInets are sufficiently reliable. We therefore designate the operation of interstate interconnecting ESInet facilities as a covered 911 service and subject the associated facilities supporting interconnection to IP path diversity requirements.[214]

Reliability Requirements

Reasonable Measures

We adopt our proposal to make the new classes of IP-based CSPs identified above subject to 911 reliability requirements.[215] This will require them to take reasonable measures to provide reliable 911 service with respect to physical diversity, network monitoring, and operational integrity.[216] The structure of our framework provides CSPs with regulatory clarity and enables them to implement consensus-driven IP reliability best practices that marshal the flexible capabilities of IP architecture, such as automatic rerouting and geodiversity.[217] In addition, our framework preserves flexibility such that CSPs may satisfy the reliability requirement by performing each element of the reliability benchmarks or by adopting alternative measures in lieu of any specifically-delineated benchmark that are reasonably sufficient to mitigate the risk of failure. A CSP also may certify that one or more benchmarks are inapplicable to its network.

Expanding the reasonableness requirement to additional IP-based CSPs critical to NG911 fulfills the Commission's longstanding commitment to keep the 911 reliability framework current as the technology landscape evolves. The Commission has advised for years that, when appropriate, it would expand the rules "to cover new best practices or additional entities that

---

[214] We disagree with Intrado that interstate interconnecting ESInet facilities would lack visibility into their traffic for the same reasons explained in the context of major IP transport: namely, voice providers are already under obligations to know what traffic they are receiving from upstream providers. *See* Intrado Comments at 20.

[215] Appendix A (§ 9.19(b)).

[216] The physical diversity and operational integrity benchmarks will only apply to specified classes of NG911 and IP CSPs. We expect our amendments to regulatory text will provide clarity for CSPs as to which benchmarks they must certify. Nevertheless, we will retain the option for CSPs to certify that a benchmark is not applicable to their services or facilities.

[217] *See NG911 Transition Order*, 39 FCC Rcd at 8221-22, para. 185 & n.546 ("NG911 materially reduces the number of 911 outages by improving network availability and reliability as IP allows for greater redundancy. It provides greater geodiversity for PSAPs – no longer will there be a single point of failure at a selective router.") (internal citation omitted).

provide NG911 capabilities[.]"[218] We conclude that extending the reasonableness requirement to additional IP-based CSPs is a logical and timely step that aligns the updated 911 reliability framework with the NG911 networks increasingly in use and strengthens the overall integrity of the nation's 911 system. We also conclude that it is reasonable for NG911 CSPs to protect network reliability by adhering to prevailing industry standards.[219] Our benchmark framework provides a consistent basis for the Bureau to exercise its delegated authority to investigate and validate the reliability of 911 networks based on CSPs' certifications, and it enables the Bureau to monitor trends in these networks in order to identify and proactively mitigate potential risks to 911 service.[220]

Our approach also facilitates state, local, and tribal planning and control of 911 networks and implementation of NG911 in their jurisdictions. For example, in NG911 systems, a state 911 Authority may decide that paying for diverse IP transmission paths to remote or rural PSAPs is cost prohibitive, and that a preferred approach would be to implement NGCS policy routing functions that automatically reroute calls to available PSAPs when one PSAP goes offline.[221] Even at this early stage of NG911 deployment, this NGCS policy routing technology has already worked to connect people to 911 during a natural disaster when the local PSAP's communication connections were disabled.[222] We expect 911 Authorities to take advantage of these new capabilities as cost-effective reliability solutions, and we expect to find these capabilities to be

---

[218] *2014 Reliability NPRM*, 29 FCC Rcd at 14221, para. 40 (quoting *911 Reliability Order*, 28 FCC Rcd at 17533, para. 159).
[219] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2690, para. 56 & n.118 (citing *CSRIC VI WG 1 Report* at 115, 122, 124).
[220] *See* 47 CFR § 0392(h).
[221] *NG911 Transition Order*, 39 FCC Rcd at 8223, paras. 188-189 (NG911 policy routing "will reduce 911 call failures" because "[i]n legacy 911 networks, selective routers must be relatively close to the PSAPs they serve, whereas in NG911, traffic can be easily rerouted to servers and locations outside the affected area, providing more resiliency and redundancy in disaster situations," and because NG911 policy routing allows "911 calls to be re-directed or redistributed among PSAPs based on outages, maintenance, or other emergencies.").
[222] North Carolina 911 Board, 911 Call and Data Interoperability Resiliency Compendium at 2, (Apr. 2026), https://content.govdelivery.com/attachments/NC911BOARD/2026/04/01/file_attachments/3604080/NC911%20Board%20Resiliency%20Compendium%20V1%202026.04.01_FINAL.pdf (stating that during Hurricane Helene, North Carolina's ESInet allowed for "the seamless delivery of 911 calls outside the impacted area to other PSAPs for call processing"); *see also* Sophia Fox-Sowell, *North Carolina officials say next-generation 911 network withstood Hurricane Helene*, (Oct. 21, 2024), https://statescoop.com/north-carolina-next-generation-911-hurricane-helene/.

reasonable alternatives in those circumstances—as the Commission has judged similar technologically reasonable alternatives in the past.[223] Accordingly, our 911 reliability framework affords 911 Authorities flexibility to fashion such solutions as part of their contracts with CSPs and based on specific local conditions.[224]

Public safety commenters strongly support the Commission's overall approach, stating, for example, that it "fully aligns with sound public policy by giving the Commission reasonable oversight of NG911 network reliability without micromanaging the construction and operation of the various aspects of the network."[225] We disagree with those commenters that suggest replacing our 911 reliability framework with a requirement for CSPs to stay compliant with reliability standards developed by external standards bodies, such as NENA and ATIS.[226] Commenters advocating this view do not agree on which external standards the Commission should endorse, nor do they explain why those standards are preferable to the Commission's reliability framework, which draws heavily from cumulative recommendations made by CSRIC. We believe CSRIC is an ideal source of guidance because it is dedicated to NG911 reliability and other public safety communications issues, and its membership includes expert representatives from major service providers, industry trade groups, manufacturers, government agencies, public safety interest groups, and industry- and public safety-led standards bodies.[227] CSRIC's work is collaborative and consensus-driven, and so the best practices it recommends

---

[223] Verizon Comments at 15 (stating that the Commission articulated reasonable alternative measures for legacy 911 in 2013 and similar clarity is needed for NG911); *911 Reliability Order*, 28 FCC Rcd at 17510, paras. 98-99 (reasonable alternative measures could include spreading out equipment and trunks within a single building to "provide a modest level of diversity" and that "may be considered reasonably sufficient to mitigate the risk of insufficient physical diversity, depending on the facts").

[224] *911 Reliability Order*, 28 FCC Rcd at 17497, para. 62 ("Because the decision whether to order diverse access through multiple selective routers, or the functional equivalent, typically rests with the PSAP and is driven by budgetary and other local concerns, we agree that service providers should not be inflexibly required to install costly, redundant circuits where a PSAP has not ordered that level of service.").

[225] Texas 9-1-1 Entities Comments at 3; *see also*, *e.g.*, APCO Comments at 6 ("These practices are essential to ensuring that 9-1-1 systems remain resilient, secure, and capable of functioning during emergencies when they are needed most."); NENA Comments at 12, 21; City of Coconut Creek, FL July 21, 2025 Comments at 1; COPUC Comments at 9; CCOA Reply at 3 ("The proposed changes to require that CSPs provide physical diversity, operational integrity, network monitoring, and interoperability for their covered 911 facilities are necessary and critical to the foundation on which NG911 core services will operate."); NASNA Comments at 6.

[226] *See* iCERT Comments at 14-15; Comtech Comments at 16.

[227] *See*, *e.g.*, *CSRIC VI WG 1 Report* at 11-15 (listing contributors, including multiple NENA representatives). The report considers and incorporates ATIS standards throughout. *See generally id*.

generally involve aspects of service that most providers are already adopting consistently.[228] Using the Commission's rulemaking process to periodically update reliability standards ensures transparency and affords CSPs the opportunity to help inform our actions. The Commission will continue to monitor the root causes of 911 outages, the reliability practices that CSPs report that they have implemented, and CSRIC's future recommendations regarding 911 reliability best practices, and will consider updating the 911 reliability framework as necessary.

Benchmarks

Physical Diversity

We update the physical diversity benchmark and several related definitions to reflect the prevailing mechanisms by which IP networks can and should provide reliable traffic delivery through physically diverse functional elements.[229] Specifically, we require IP-based CSPs to certify, for all the 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. This is a modification of the benchmark proposed in the *NG911 Reliability FNPRM*, which would have required CSPs to *eliminate* all single points of failure rather than mitigate them. CSPs meeting this new benchmark are required to mitigate these risks in both the physical and logical layers of 911 transport. CSPs may meet the benchmark through alternative measures if appropriate, or they may certify that the diversity benchmark is inapplicable to their networks. We also clarify that CSPs may secure dedicated diverse backup paths outside of their engineered networks, including MPLS transport, cloud-based path redundancy, or VPN services over the public Internet, and implement logical diversity such as through multi-homing, to mitigate the risk of single points of failure.

Updates to the physical diversity benchmark. We find that updating the physical diversity

[228] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2673-74, para. 10.
[229] Appendix A (§ 9.19(c)(1)).

benchmark is necessary to ensure that our reliability framework keeps pace with the technological realities of IP-based NG911 networks. These networks, when engineered properly, can achieve highly resilient call delivery, and requiring them to incorporate prevailing reliability practices ensures CSPs will implement these resiliency features consistently. Updating the benchmark also streamlines the reliability certification process for IP-based CSPs, because they will no longer need to provide detailed descriptions of their IP-based mitigation practices as "alternative measures" to an inapplicable legacy standard.[230]

Mitigating single points of failure. Both legacy, circuit-switched 911 networks and IP-based NG911 networks address the risks posed by single points of failure through physical diversity, but the strategies they use to do so are fundamentally different.[231] Legacy 911 networks determine the circuits and switches that a call will traverse from its origin to its destination when the call is set up. This means that a problem in any network component along the planned route can cause the transmission to fail. Legacy networks minimize that risk by providing at least two independent sets of physically-separated circuits and switches, which eliminates the possibility that a failure of any single network element will disrupt the transmission.[232] The legacy physical diversity benchmark reflects this strategy, as it requires CSPs to certify whether they have eliminated all single points of failure along their critical 911 circuits.[233]

---

[230] We are not persuaded by Lumen's concern that the benchmark might conflict with the reliability implementations of CSPs that already have "fortif[ied] their networks." *See* Lumen Comments at 7. These CSPs likely incorporated the prevailing measures we adopt today, or they may certify their configurations as alternative measures if appropriate.

[231] In general, "physical diversity" means that data between two points in a network can be transmitted over diverse routes that do not share any common physical segments, such as fiber-optic cables, conduits, or structures, so that a single failure at any point on one of those data paths, such as a power outage, equipment failure, or cable cut, would not cause both paths to fail and disrupt the transmission of data between those points. 47 CFR § 9.19(a)(8). *See also* NENA, NENA Knowledge Base, https://kb.nena.org/wiki/SIP (last visited May 19, 2026) ("Single Point of Failure is a failure of a hardware or software component or sub-system which causes a system to fail.").

[232] *See*, *e.g.*, *911 Reliability Order*, 28 FCC Rcd at 17504, para. 83 ("Physical diversity, sometimes called route diversity, means that two circuits follow different routes separated by some physical distance so that a single failure such as a power outage, equipment failure, or cable cut will not result in both circuits failing."); 47 CFR § 9.19(a)(8) (defining physical diversity); NENA Comments at 23 ("When considering physical diversity, conventional wisdom within telecom has always been 'two of everything at each of two sites.'").

[233] 47 CFR § 9.19(c)(1)(i).

In contrast, NG911 and IP networks create physical diversity primarily by being capable of automatically and dynamically rerouting 911 traffic throughout a web of alternate paths.[234] The IP routers or nodes in the network decide where to forward packetized call data based on internal routing tables, connected by IP paths and node links.[235] If a router or node detects a failure in the primary path, it automatically and instantly reroutes the call along a secondary path. This capability means that, "[i]f there is any path between two points in an IP network, then the network will automatically find and use that path."[236] Because NG911 networks can deliver traffic along numerous possible routes, physical separation of individual IP paths may not be essential in all locations to achieve reasonable network reliability.[237] Instead, NG911 networks create resiliency by maintaining redundant routers or nodes and node links that automatically failover to redundant elements and paths. These networks typically space redundant elements widely in different geographic locations and different physical facilities to protect them from failing due to the same external event.[238] These networks practice load balancing by dynamically distributing network traffic across multiple available databases or call processing facilities so that the network maintains continuity of service to prevent redundant elements from becoming overwhelmed even when traffic surges.[239] The physical diversity benchmark we adopt today is broadly worded to reflect these prevailing approaches while remaining technology-neutral so as to provide legacy and NG911 CSPs a high degree of flexibility when choosing their implementation strategies.

The specific capabilities we incorporate into the physical diversity benchmark—automatic

---

[234] Intrado Comments at 20 ("NG911 routing . . . presents a spiderweb-like, nearly infinite matrix of physical and virtual connections over which disassembled packets traverse.").
[235] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2693, para. 62.
[236] NENA Comments at 10. An IP network's ability to automatically detect failures and reroute traffic is sometimes referred to as "self-healing." *See*, *e.g.*, USTelecom Comments at 7.
[237] USTelecom Comments at 7-8; NENA Comments at 10.
[238] *See*, *e.g.*, BRETSA Reply at 3 ("With geographically diverse network paths, loss of service on a single network path due to an equipment failure or the severing of a fiber line by a backhoe, for example, will not disrupt service. In the event one of two diverse paths is disrupted, all traffic will flow across the second path. *Network path diversity significantly reduces the likelihood of an outage*.") (emphasis in original); USTelecom Comments at 7-8.
[239] *2014 Reliability NPRM*, 29 FCC Rcd at 14227, para. 45 & n.107; *NG911 Reliability FNPRM*, 40 FCC Rcd at 2693, para. 62.

rerouting and failover across geographically-distributed routing facilities, transport nodes, and node links, supported by load balancing—are well-recognized strategies that are synonymous with sound IP architecture. In its 2013 *Derecho Report*, the Bureau found that NG911 networks would likely have mitigated the 911 outages caused by the 2012 derecho due to the resiliency and redundancy these networks provide using IP routers with automatic fail-over; automatic rerouting; and diverse IP paths.[240] When CSRIC updated its best practice recommendations for NG911 in 2019, it assumed that the design of transitional and end-state ESInets would ensure "all network elements and transport facilities are deployed with redundancy."[241] CSRIC explained that "[t]ypically, network redundancy is achieved through the addition of alternate network paths, which are implemented through redundant standby network elements, routers and switches. When the primary path is unavailable, the alternate path can be instantly deployed to ensure continuity of network services."[242]

Our benchmark also reflects CSRIC's best practice recommendations for NG911 service providers. CSRIC recommends that service providers ensure the geographic separation of network redundancy facilities; dedicated, geo-diverse, and redundant IP connection points; functional redundancy and geographic diversity for critical network elements; physical and geographic redundancy for critical facilities links; diverse routing from OSPs to the ESInet; and redundant connectivity from the ESInet to PSAPs.[243] It further recommends that service providers manage "critical network elements and architecture that are essential for network connectivity and subscriber services considering . . . functional redundancy and geographical diversity"; "ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical

---

[240] *Derecho Report* at 44. *See also 2014 911 Reliability NPRM*, 29 FCC Rcd at 14227, para. 45 ("We also believe that the [CSP reliability] certification should indicate whether a service provider's IP-based 911 architecture is geographically distributed, load-balanced, and capable of automatic reroutes to backup equipment in the event of a hardware, network, software or database failure.").
[241] *CSRIC VI WG 1 Report* at 51.
[242] *Id*.
[243] *Id.* at 86, 87, 109, 114, 122, 124; *see also 2020 Best Practices Public Notice*, 35 FCC Rcd at 13179-81 (reminding CSPs to adopt industry best practices, including diverse data paths and call rerouting).

facilities in the same physical path)"; use load balancing to "ensure that the utilization on either node is less than half of each node's capacity so that if one node fails the other node will absorb the load"; and "plac[e] and maintain[] 9-1-1 . . . IP based networks over diverse interoffice transport facilities (e.g., geographically diverse facility routes), automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof."[244]

Commenters identify other logical and physical diversity mitigation strategies, including the use of diverse MPLS transport, cloud-based services, or the public Internet as automatically re-routed backup paths.[245] Although the record demonstrates that these strategies can make NG911 more resilient, we decline to specify that any of them is a benchmark practice at this time.[246] CSRIC has not identified these practices as necessary to all NG911 implementations, and we are concerned that requiring them could be overly prescriptive or cost prohibitive in some scenarios. NG911 networks vary substantially in size, geography, legacy configurations, and available commercial infrastructure, and the benefits of these measures may depend on technical and economic factors that differ across jurisdictions. Instead, we identify these approaches as permissible mitigation strategies and strongly encourage CSPs to adopt them where appropriate to enhance resiliency. This approach preserves flexibility for providers to tailor their reliability solutions to their own operational environments while ensuring that foundational NG911 reliability standards remain clear, achievable, and technologically

---

[244] FCC, CSRIC Best Practices 13-10-06, 13-10-507, 13-12-322, 13-12-3277, and 13-9-0566, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/about_data (last visited May 19, 2026); *cf.* NENA Comments at 22 ("While there are certainly circumstances where load balancing is a characteristic that is built into systems, generically, IP networks don't perform load balancing.").

[245] *See*, *e.g.*, NENA Comments at 9-11, 20; Brian Rosen Reply at 5. Intrado suggests replacing the physical diversity benchmark entirely with a requirement for CSPs to secure backup paths via other providers' networks. *See* Intrado Comments at 21 ("[T]he standard could be to require a CCSP to procure a minimum number of diverse connections from different network providers with a minimum number of points of interconnection in geographically diverse locations.").

[246] *See*, *e.g.*, USTelecom Comments at 8 ("In many cases, modern networks inherently offer greater reliability, not because of any single element such as physical route diversity, but because of a combination of design strategies tailored to specific network environments and operational needs.").

neutral.[247]

We leave unchanged the physical diversity requirements for legacy CSPs, but take this opportunity to revise the requirements for brevity and clarity.[248] Legacy CSPs may continue to satisfy the physical diversity benchmark by ensuring that all covered 911 circuits in their network are tagged and physically diverse such that no network or facility element constitutes a single point of failure and by conducting annual diversity audits. In addition, both legacy and IP CSPs retain the option to implement alternative measures to the benchmarks that mitigate the risks of a lack of physical diversity or to demonstrate that the physical diversity requirements do not apply to one or more covered portions of their networks.[249]

Definitions. To facilitate compliance with the physical diversity benchmark, we update the definition of "physically diverse" to incorporate the IP benchmark capabilities that we describe above, as well as to reference "paths" in addition to "circuits," so that the definition accurately reflects common terminology for IP transport elements.[250] We also adopt new definitions for the terms "geographically distributed" and "load balanced" based on their meanings as described in the *NG911 Reliability FNPRM* and as previously recognized by the Commission.[251] We find that adopting functional definitions of these terms will explain important technical concepts reflected in the physical diversity benchmark, provide guidance to CSPs seeking to implement the benchmark, and assist 911 Authorities and other stakeholders responsible for overseeing the

---

[247] Verizon Reply at 4 ("[C]ommenters broadly recognize the need for flexibility in applying any new 'conformance' and 'alternate measures' certification standards.").
[248] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2693, para 62.
[249] We reject Lumen's claim that the benchmark imposes inescapable requirements on CSPs. *See* Lumen Comments at 6. While it reflects best practices that are feasible in typical NG911 deployments and should be followed in most cases, CSPs may certify alternative measures if necessary.
[250] Appendix A (§ 9.19(a)(8)).
[251] Appendix A (§ 9.19(a)(10), (11)); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2693, para 62 & n.133 (quoting 2014 *Reliability NPRM*, 29 FCC Rcd at 14227, para. 45 & n.106 ("[N]etwork architectures utilizing… databases in different geographic locations . . . will be more reliable and resilient than those that route all calls through a single active database . . . .")); *id*. at 2693, para 62 & n.134 (quoting 2014 *Reliability NPRM*, 29 FCC Rcd at 14227, para. 45 & n.107 ("A 911 network is 'load balanced' if call volume is dynamically distributed among all available databases or call processing facilities rather than concentrated in one location. Calls assigned to each database should be automatically rerouted to the other in the event of a fault with the primary route. Furthermore, if two or more PSAPs share the same 911 service provider and rely on each other as a backup PSAP for rerouting of 911 calls, the 911 service provider should consider assigning each PSAP to a different primary routing database.")).

provision of reliable 911 service. Accordingly, we adopt the following definitions:

- *Physically diverse*. Circuits or paths are physically diverse if they provide more than one physical route between end points with no common points where a single failure at that point would cause both circuits or paths to fail. Circuits or paths that share a common segment such as a fiber-optic cable or circuit board are not physically diverse even if they are logically diverse for purposes of transmitting data. IP routers, transport nodes, and node links create physical diversity if these elements are redundant, geographically distributed, load balanced, and capable of automatic failover and rerouting to redundant elements sufficient to reasonably mitigate the risks of single points of failure.
- *Geographically distributed*. 911 network architecture is geographically distributed if 911 traffic can be delivered through more than one covered 911 circuit or path in different geographic locations in different physical facilities.
- *Load balanced*. 911 network architecture is load balanced if call volume is dynamically distributed among multiple active databases or call processing facilities to accommodate changes in traffic volume.

The Commission asked in the *NG911 Reliability FNPRM* whether it should define geographic distribution more specifically to mean the housing of functional elements in different cities or states.[252] We decline to further specifically define geographic distribution at this time. Any fixed standard for geographic distribution could prove too prescriptive or invalidate some existing IP network architectures. We also expect that national NG911 CSPs naturally will space their routing elements widely across different regions and that state and local 911 Authorities will negotiate the placement of NG911 facilities within their jurisdictions to maximize reliability. We therefore find it unnecessary at this time to define geographic diversity with greater specificity than as proposed in the *NG911 Reliability FNPRM*.

[252] *Compare*, *e.g.*, NENA Comments at 22 (routing elements should be distributed widely so that they are not affected by the same weather events), *with* Comtech Comments at 18 ("[G]eographic diversity is a continuum and is inherently more subjective (*e.g.*, whether network elements are sufficiently far apart geographically . . . .").

The physical diversity benchmark applies to "covered 911 circuits and paths."[253] Accordingly, we update the definition of this term as well so that it includes the IP-based transport facilities we newly-designate today as covered facilities. Specifically, we adopt the *NG911 Reliability FNPRM*'s proposal specifying that the IP paths covered by our 911 reliability framework include major IP transport paths, IP 911 traffic aggregation paths, interstate interconnecting ESInet facilities, and IP traffic paths from NGCS facilities to PSAPs.[254]

We also include all IP transport paths that originate at an NG911 delivery point or ESInet point of interconnection and terminate at the last routing facility before reaching the PSAP, and all equipment necessary for the delivery of 911 traffic to the PSAP, including any trunks, circuits, or paths to and from NGCS facilities and the ESInet transmission network necessary for routing and caller location information to the PSAP(s), and any intermediate paths in the chains of delivery.[255] These are appropriate segments of NG911 networks to receive physical diversity protections because they encompass the processing and transport facilities at which 911 traffic is most heavily concentrated. They also are the elements in NG911 networks that are functionally equivalent to the critical circuits in legacy networks that are subject to the legacy physical diversity requirement.[256] We include in our definition of IP 911 covered paths the transport routes emerging from or terminating at NG911 transitional architecture, such as an LSRG or LPG. We reiterate that transitional mixed TDM-IP facilities should apply legacy or IP reliability benchmarks as appropriate to TDM paths or IP paths.

---

[253] Appendix A (§ 9.19(c)(1)).

[254] Appendix A (§ 9.19(a)(5)); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2694, para. 65 (stating that "IP traffic paths from NGCS facility capabilities (when provided directly to PSAPs)" are covered 911 paths under the proposed rules); *id*. at 2695, para. 66 (stating that "major transport paths and 911 aggregator networks" are covered 911 paths under the proposed rules); *id*. at 2690, para. 55 (stating that "interconnection facilities should be treated as critical facilities" subject to reliability requirements under the proposed rules).

[255] Palmetto Broadband Coalition, a group of 15 South Carolina RLECs, argues that ESInet operators are not adequately covered by the prior 911 reliability rules. Palmetto Broadband Coalition Reply at 1-2 & n.4; *id.* at 2-3 ("We are concerned about the current lack of clear and consistent rules applicable to ESInet providers like Comtech" which has argued that it provides "information services" and is therefore not subject to regulation by the state public utilities commission). *See also* Home Telephone Comments at 12.

[256] *See* 47 CFR § 9.19(a)(5). The *NG911 Reliability FNPRM* proposed to include the ESInet and NGCS by reference to them as "functional equivalents", but the definition we adopt today defines critical IP paths more explicitly by their location and function to provide regulatory clarity. *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2694, para. 65; *id.* at 2728 (proposed language in 47 CFR § 9.19(a)(5)).

To avoid any ambiguities going forward, we remove language from the proposed IP covered 911 paths definition referencing "central offices," and add language covering "circuits," in order to respond to concerns from CCOA and NASNA.[257] CCOA states that legacy providers of paths to PSAPs have argued that the 2013 circuit auditing and diversity benchmarks do not apply to them.[258] NASNA adds that the Commission's proposed definition of critical 911 paths to PSAPs is inadequate to capture the full range of ESInet traffic.[259] Updating this language is important both for current clarity where ILECs continue to route 911 traffic to PSAPs through legacy central offices and networks and for modernized and upgraded networks as legacy central offices are retired and replaced by IP-based paths.

We decline to exclude intermediate paths in the chain of delivery from our definitions of covered IP paths, as this would allow providers to circumvent our reliability regime merely by handing off traffic to another entity.[260] However, we reiterate that IP 911 traffic aggregators may make the same certifications as ESInet operators about which underlying transport providers or MLPS vendors they have service level agreements with, the extent to which those providers are sharing network data or delivering path diversity as promised, and any multi-homing or other measures the IP 911 aggregators are implementing to ensure IP path diversity. The IP diversity benchmark we adopt today, which incorporates geo-diversity per the CSRIC best practices, provides robust reliability that should reduce the risk of 911 outages resulting from fiber cuts—and particularly instances where a fiber cut in a single location results in a 911 outage across an entire state or region. If the Commission receives reports that underlying transport providers are not reasonably cooperating to ensure 911 reliability, and that this lack of cooperation is resulting

---

[257] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2728 (proposed rule 47 CFR § 9.19(a)(5)).
[258] CCOA Reply at 4 ("This FNPRM provides an opportunity to close what one CSP claims is a 'gap' in the diversity audit process. The 'gap' results from use of the phrase 'central office that serves the PSAP.'").
[259] NASNA Comments at 3 ("NASNA recommends that the term 'trunk' be replaced with the term 'circuit' in the covered service provider definition . . . . While the IP-equivalent to TDM trunks are SIP trunks, there are a lot of other services and protocols that will traverse ESInet networks besides SIP traffic[.]").
[260] Intrado Comments at 19; *see also Massachusetts Ex Parte* at 4 ("[W]hen the combined traffic of multiple OSPs is not delivered directly but is instead delivered to a second aggregator in the call delivery path where it is aggregated with the second aggregator's combined traffic, the risk of an outage affecting the delivery of each OSP's traffic increases at least two-fold at the second aggregation point.").

in 911 outages, we can revisit our CSP categories at that time.

The updated IP physical diversity benchmark and associated definitions have strong support from public safety commenters.[261] CCOA, for example, believes the benchmark strengthens reliability by requiring CSPs to "provide physical diversity" that is "necessary and critical to the foundation on which NG911 core services will operate."[262] Commenters note the importance of adding a requirement for geographic diversity, because it protects 911 service against more causes of outages than simple physical diversity.[263] Commenters also support retaining the physical diversity benchmark for legacy providers, which we do.[264] We decline Lumen's suggestion to modify the benchmark for IP path diversity by identifying auditing and tagging as presumptively reasonable, because auditing and tagging are legacy TDM reliability practices that do not necessarily measure the inherently more-resilient geodiversity of IP networks.[265] However, CSPs may certify to auditing and tagging their IP paths to ensure complete physical route diversity as an alternative measure. We also decline to adopt one commenter's suggestion to require legacy CSPs to produce new types of data during diversity audits of critical circuits and to require all OSPs to perform diversity audits as well.[266] These changes would greatly expand the scope and burden of the diversity benchmark, and there is insufficient evidence in the record to suggest that such an expanded requirement would provide commensurate benefits.

---

[261] *See*, *e.g.*, NASNA Comments at 7; BRETSA Reply at 3; NENA Comments at 20 ("Network paths must be geographically diverse."); APCO Comments at 6; CCOA Reply at 4; COPUC Comments at 10; Brian Rosen Reply at 2.

[262] CCOA Reply at 3 ("Physical diversity of covered 911 facilities is of utmost importance.").

[263] *See*, *e.g.*, COPUC Comments at 10 ("It does very little good to have two transport circuits for redundancy, both of which run through the same conduit or along the same roadway where they can both be cut by the same construction worker."); CCOA Reply at 4; BRETSA Reply at 3 ("Geographic Diversity Is the *Sine Qua Non* of Network and Service Reliability."); NENA Comments at 20 ("Network paths must be geographically diverse."); Brian Rosen Reply at 2; USTelecom Comments at 9 ("[G]eographic diversity . . . may offer greater reliability than physically diverse fiber routes serving the same region."). *See also* Comtech Comments at 18 (noting the importance of distinguishing geographic diversity from physical diversity).

[264] NASNA Comments at 7.

[265] Lumen Comments at 6 (urging the Commission to "maintain the current balance promoted by section 9.19 of its rules, where the adherence to CSP physical circuit diversity is safeguarded by circuit auditing and CSPs' annual reliability certifications").

[266] BRETSA Reply at 3-5.

Support for the diversity benchmark from service providers is mixed, but several providers oppose the benchmark language proposed in the *NG911 Reliability FNPRM* in whole or in large part because it would have required IP physical diversity measures that "eliminate all single points of failure."[267] They argue that such a requirement would be cost prohibitive or infeasible, because NG911 networks reroute calls dynamically without preplanning or tracing call routes, and packetized call data may sometimes converge at single points without the provider being aware.[268] We acknowledge that eliminating all single points of failure is not presently a design goal of typical NG911 deployments, and we have revised the IP physical diversity benchmark accordingly to require reasonably sufficient *mitigation* of single points of failure.

In response to Intrado's concern that upstream or downstream providers could interfere with its performance of the benchmark, we clarify that a CSP's compliance depends solely on the CSP's configuration and operation of facilities under its control.[269] We emphasize, however, that CSPs must take full responsibility for meeting the benchmarks, or implementing reasonable alternative measures, and that nonperformance with respect to facilities under the CSP's control cannot be justified by the practices or limitations of third parties. The 911 reliability framework, together with the Commission's NG911 transition framework, synergistically afford providers and 911 Authorities the flexibility and control they need to plan and deploy seamless NG911 connectivity. To use Intrado's hypothetical example, a NGCS CSP and 911 Authority that

---

[267] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2729; *see also*, *e.g.*, Motorola Comments at 7-8 (arguing that, if this language were corrected, the resulting benchmark "would accomplish the FCC's goal of ensuring that 'critical paths established by CSPs [are] geographically diverse, load-balanced, and capable of automatic failover to the backup element . . . and automatic reroutes to redundant paths in the transport layer in the event of path failure,' while recognizing the operational realities of NG911 networks."); iCERT Comments at 15 (expressing support if the requirement to eliminate single points of failure were removed); Comtech Comments at 18 (same); USTelecom Comments at 7-8 (any benchmark update should "preserve flexibility for OSPs and CSPs to determine the most effective means of ensuring resilience in their own networks"); Lumen Comments at 5.

[268] Lumen Comments at 4-7; Intrado Comments at 21 ("[A] CSP has no way to know if these geographically diverse and provider-diverse connections could eventually experience packet convergence at a single point of failure, making it effectively impossible to certify truthfully to the Commission that there is no single point of failure."); Motorola Comments at 6-7 (The "dynamic IP routing of 911 calls . . . prevents precise tracing of each physical route that calls may take within the network.").

[269] *See* Intrado Comments at 16-17; *id*. at 21-22 ("[A]n NGCS provider can provide OSPs with an interconnection guide and recommendations for redundant connectivity, load balancing, and advance routing, but it cannot force the OSP to purchase or configure a particular architecture."). *See also* Verizon Comments at 14 (suggesting the 911 Authorities' readiness could impact OSPs' performance).

provide two entry points to an ESInet to support geographic diversity can require OSPs to deliver 911 traffic to both POIs in a format that is compatible with the CSP's network configuration.[270]

Other IP reliability measures. For clarity, the updated benchmark does identify several examples of diverse IP paths that CSPs may adopt, but it does not require that any specific one, or all, of them be implemented.[271] Significant developments in network design and operational practices in recent years have allowed modern NG911 and IP networks to employ additional strategies to increase the reliability of call transmission.[272] Providers may create additional geo-diverse redundancy beyond their own engineered paths by securing backup paths from third-party cloud- or Internet-based solutions.[273] These solutions typically connect into the CSP's network through secure, SIP-capable interfaces that automatically activate if the CSP's primary path fails. The services then deliver 911 traffic through the cloud or over the public Internet using a VPN for security. Third-party services may handle call delivery, or they may provide a routing solution and hand off 911 traffic to a non-failing portion of the CSP's network or to another CSP for delivery. CSPs also may arrange backup paths over the public Internet without using third-party services.[274] We note that using the public Internet may expose 911 traffic to risks such as possible Denial of Service (DoS) and Telephony Denial of Service (TDoS) attacks, making enhanced security protections advisable. While we do not mandate such measures today, we encourage OSPs and CSPs relying on the public Internet for backup purposes to implement common-sense security measures to protect the reliability of 911 traffic.[275]

---

[270] *See* Intrado Comments at 21; 47 CFR § 9.32 ("A 911 Authority may designate one or more NG911 Delivery Points where [OSPs] must deliver 911 traffic to the ESInet[.]"); 47 CFR § 9.29(a) (At Phase 1, OSPs must "[d]eliver all 911 traffic . . . in the IP-based SIP format requested by the 911 Authority"). We remind providers that, if they cannot conform to a benchmark practice, they may implement reasonable alternative measures. *Cf.* Intrado Comments at 17-18.

[271] Appendix A (§ 9.19(c)(1)(i)).

[272] USTelecom Comments at 8 ("In many cases, modern networks inherently offer greater reliability, not because of any single element such as physical route diversity, but because of a combination of design strategies tailored to specific network environments and operational needs.").

[273] USTelecom Comments at 8.

[274] *See*, *e.g.*, NENA Comments at 10 ("To maintain very high reliability, it is essential that there be some paths that use the public internet, possibly with a [VPN], and follow Commonly Accepted Standards for NG9-1-1 security.").

[275] NENA Comments at 10-11 (noting DoS and TDoS attack risks and advising that CSPs' network implementations "should not rely exclusively on the public internet to connect to an ESInet or NG9-1-1 facility"); *CSRIC VI WG 1 Report* at 109 ("Network Operators that utilize the Public Internet for signaling, transport, or maintenance

NG911 providers may also secure access to dedicated third-party high-capacity physical transport that is geographically diverse from their own facilities, such as MPLS networks that transport data between nodes based on short path labels, which avoids complex lookups in routing tables.[276] CSRIC notes the use of MPLS transport as an optional method to increase redundancy in ESInets but does not designate it a high-priority capability for all CSPs.[277] We find that CSPs may use dedicated diverse private facilities such as MPLS, cloud-based path redundancy, or VPN services over the public Internet, or equally secure industry protocols as additional automatically re-routed backup paths.

CSPs may also mitigate the risk of internal network failures by employing various forms of logical diversity.[278] Logical diversity is the use of multiple, independent routing instructions or virtual paths through an IP network.[279] Unlike physical and geographic diversity, which require network facilities to be separated by physical space, logical diversity can operate within shared infrastructure and relies on independent routing logic to bypass failures in a network's processes.[280] Multi-homing is a form of logical diversity used in some NG911 networks.[281] It involves connecting critical network elements to multiple independent upstream networks or service providers simultaneously. This configuration establishes multiple distinct routing paths

---

communications should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).").

[276] NENA Comments at 9-10 ("Many NG9-1-1 deployments depend on a single carrier's MPLS network to interconnect OSPs, NGCS components and PSAPs."); Brian Rosen Reply at 5 (referring to "NGCS operator[s] who purchase MPLS paths to form their ESInets"); *see also* NENA, NENA Knowledge Base, https://kb.nena.org/wiki/MPLS_(Multiprotocol_Label_Switching) (last visited May 19, 2026).

[277] FCC, CSRIC Best Practices 13-12-3258, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/about_data (last visited May 19, 2026) ("Public Safety ESInets may use diverse private facilities or their functional equivalent (e.g., MPLS, generic routing encapsulation (GRE) tunneling, virtual private network (VPN), or equally secure industry protocols) and where appropriate and supported by service level agreements.").

[278] *See*, *e.g.*, *CSRIC VI WG 1 Report* at 122 ("Network Operators . . . and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links.").

[279] *See 911 Reliability Order,* 28 FCC Rcd at 17504, para. 83 ("[T]wo circuits that are modulated onto two wavelengths are logically diverse. If they are then placed onto two physically separate optical fibers whose routes do not meet, they are also physically diverse . . . . If, instead, they are placed onto the *same* optical fiber, they are no longer physically diverse, but they retain their logical diversity.").

[280] *See* 47 CFR § 9.19(a)(8) ("Circuits that share a common segment such as a fiber-optic cable or circuit board are not [p]hysically diverse even if they are logically diverse for purposes of transmitting data.").

[281] *See*, *e.g.*, *CSRIC VI WG 1 Report* at 109 (recommending as a best practice that service providers "who deploy next generation signaling networks should consider industry guidelines for logical diversity (e.g. multi-homing), and perform network diversification validation on a scheduled basis (e.g., twice a year)").

at the network layer, but some underlying physical infrastructure may overlap. As a result, multi-homing enhances overall network reliability and resiliency against outages, congestion, or localized network disruptions. CSRIC recommends the use of logical diversity strategies like multi-homing in addition to physical diversity where feasible.[282]

Operational Integrity

We adopt the *NG911 Reliability FNPRM* proposal to (1) update the "backup power" benchmark so that it applies to IP-based CSPs that operate multi-OSP LNGs, multi-OSP LISs, or covered NGCS functional elements, and (2) change the benchmark name to "operational integrity" to better reflect the methods by which IP networks protect service continuity.[283] We additionally specify that operators of covered LSRGs, ESGWs, and LPGs are subject to the benchmark, consistent with our determination in this *Order* that these elements are essential to transitional NG911 networks.[284] IP CSPs meet the benchmark if their covered facilities have the capability to ensure continuity of services via an uninterruptible and continuous power supply and automated switchover to geographically diverse backup facilities and configurations sufficient to prevent service disruption. For legacy CSPs, the backup power requirements for central offices remain the same substantively, but we implement minor updates to improve readability. All legacy and IP CSPs also retain the option to achieve operational integrity through alternative measures.[285]

Extending the operational integrity benchmark to CSP operators of covered LNGs, LISs, LSRGs, ESGWs, LPGs, and NGCS functional elements is appropriate because those facilities perform 911 call aggregation, routing, and delivery functions analogous to the functions performed at central offices in legacy 911 networks, to which the 2013 legacy backup power

---

[282] *See*, *e.g.*, *id.* at 122 ("Network Operators . . . and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links.").
[283] Appendix A (§ 9.19(c)(2)).
[284] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2696, paras. 69-70.
[285] 47 CFR § 9.19(c)(2)(ii).

benchmark applies.[286] These functions are essential to NG911 connectivity, and their failure can disable the transmission of 911 traffic across entire communities or even large areas of the country.[287] However, we do not extend this benchmark to CSP providers of major IP transport facilities or IP 911 traffic aggregation facilities, for which geographically diverse failover capability may not be practical and supplying continuous backup power is likely to be inapplicable or unduly burdensome. While we find the operational integrity benchmark to be inapplicable to these CSP categories, we emphasize that they remain subject to the redundancy and geographic diversity elements of the physical diversity benchmark. In addition, we encourage all CSPs that have taken measures to supply continuous power and automatic switchover capability to their covered facilities to describe them in their reliability filings, which will enhance the Commission's understanding of the status of the NG911 ecosystem.

Requiring continuous power and geographically diverse automatic failover capability for applicable CSPs is consistent with CSRIC recommendations. In 2019, CSRIC VI updated its best practices for 911 service providers to recommend, for example, that service providers connect power loads at critical sites to on-site generators configured to auto-engage in the event of commercial power outages.[288] It also noted that service providers should deploy network elements in transitional and end-state NG911 networks with redundancy "for quickly swapping network operations onto redundant infrastructure in the event of an error within a network element or transmission path" and that automatic and instant failover should include "redundant standby network elements, routers and switches . . . to ensure continuity of network services."[289] CSRIC's latest best practices continue to reflect these recommendations.[290] Adding these

---

[286] *See* Intrado Comments at 22 (stating it is "generally supportive" of the proposed operational integrity benchmark, agreeing with the Commission's assessment that "the backup power benchmark becomes less significant if the Commission extends the physical redundancy requirements to NGCS facilities and location services").
[287] *See 911 Reliability Order*, 28 FCC Rcd at 17514, para. 106.
[288] *CSRIC VI WG 1 Report* at 51.
[289] *Id.* at 51.
[290] *See*, *e.g.*, FCC, CSRIC Best Practices 13-10-5058, 13-9-5204, 13-9-0657, and 13-9-1028, and 13-12-0497, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/about_data (last visited May 19, 2026) (Service providers should maintain critical communications services during power outages by supplying all critical facilities with backup power that that is on-site and engages automatically.); *id.*, Best Practices 13-9-0575, 13-9-

recommended and prevailing practices to the benchmark will help mitigate the impact of power outages on NG911 service while streamlining the certification process for IP CSPs.

Commenters are generally supportive of this proposal,[291] although some request adjustments. COPUC suggests that we extend the durations for backup power at legacy central offices beyond 24-72 hours as required under the 2013 reliability rules, but we find that there is no CSRIC best practice or basis in the record to prescribe any longer duration.[292] However, we strongly encourage CSPs operating central offices to secure additional power reserves from a variety of sources (on-site generators, mobile generators and generator delivery services, batteries, fuel reserves, etc.) to maximize their resiliency during lengthy commercial power outages. We also find it unnecessary to subject central offices that do not directly serve PSAPs to backup power standards, as one commenter suggested, because such intermediary offices likely can reroute 911 calls along physically diverse circuits or paths to reach the terminal central office that directly serves the PSAP.[293] In response to NENA's concern that CSP backup power systems too often have failed when they were needed, we remind CSPs that, by certifying their compliance with the operational integrity benchmark, they represent to the Commission that they have properly installed any necessary backup power facilities and have conducted all necessary testing and maintenance to keep them operational.[294] We also clarify that the benchmark applies only to the offices and network elements operated by the CSPs to which the benchmark applies and not to ingress or other facilities that are outside of the CSP's control.[295]

0510, 13-10-5075, and 13-10-1065 (Network elements that are essential for connectivity, including gateway servers and LISs, should be redundant and geographically diverse).

[291] *See*, *e.g.*, APCO Comments at 7; COPUC Comments at 10-11; Intrado Comments at 22 (observing that the addition of an automatic failover requirement to redundant and geo-diverse facilities reduces reliance on backup power to ensure continuity of service).

[292] The Commission based the 24-72 hour benchmark on the many comments it received on the topic in the 2013 reliability proceeding. *See 911 Reliability Order*, 28 FCC Rcd at 17518, para. 115. CSRIC currently recommends a minimum of three hours of battery reserve for central offices equipped with fully automatic standby systems. FCC, CSRIC Best Practices 13-10-0672, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/about_data (last visited May 19, 2026).

[293] COPUC Comments at 10-11.

[294] *See* NENA Comments at 22-23.

[295] *See* Intrado Comments at 22; COPUC Comments at 10-11.

Network Monitoring

As proposed in the *NG911 Reliability FNPRM*, we update the network monitoring benchmark to enable IP-based CSPs to demonstrate the reasonableness of their network monitoring measures using geographically distributed automatic disruption detection and alarm systems.[296] To qualify, the systems must protect a CSP's IP covered facilities, as well as any IP routers, transport nodes, and node links it relies on to meet the physical diversity requirement for IP covered 911 paths. Legacy CSPs may continue to demonstrate reasonable network monitoring by using physically diverse monitoring aggregation points, monitoring links, and Network Operations Centers (NOCs) and auditing the diversity of those facilities annually.[297] All CSPs retain the option to certify that they have adopted alternative network monitoring measures or to claim that network monitoring requirements are inapplicable to their networks.[298]

We adopt this modification because the 2013 network monitoring benchmark is too restrictive for IP-based CSPs. The Commission created the benchmark to respond to monitoring failures in the legacy networks of primary 911 service providers during the 2012 derecho and to implement CSRIC's recommended best practices for such providers at that time.[299] The 2013 benchmark accordingly requires CSPs to protect their monitoring functions by physically separating monitoring facilities and the links connecting them to the NOCs where data are analyzed. As we have noted, however, IP networks typically do not rely on auditing physical wire separation along each individual IP path. IP-based CSPs therefore have defaulted to certifying and describing their network monitoring practices as "alternative measures" in their filings. Providing a suitable monitoring benchmark for IP CSPs streamlines the certification process for providers, more effectively supports the reliability of NG911 networks, and improves the Bureau's ability to evaluate CSP reliability submissions.

---

[296] Appendix A (§ 9.19(c)(3)).
[297] We rename the definition "aggregation point" as "monitoring aggregation point" to distinguish the points at which monitoring data is aggregated from the points in 911 networks at which 911 traffic itself is aggregated, such as selective routers and ESInet POIs. *See* Appendix A (§ 9.19(a)(1)).
[298] 47 CFR § 9.19(c)(3)(ii).
[299] *See 911 Reliability Order*, 28 FCC Rcd at 17524-25, paras. 133-134.

We tailor this amended benchmark to reflect CSRIC's recommended practices for NG911 service providers and the prevailing architectures of modern NG911 networks. CSRIC recommends that NG911 service providers "be responsible for monitoring IP connections for transport and for capturing network traffic, generating alarms and producing other metrics for monitoring and troubleshooting outages within [ESInets], as well as those impacting the ability of an [ESInet] to deliver calls to the target PSAP."[300] This means that service providers upstream from the ESInet should "monitor for transport alarms associated with IP connections to the [ESInet]" and that, after traffic reaches the ESInet POI, service providers should "be able to detect when IP connectivity to the PSAP, or IP connectivity between the first routing element in the [ESInet] and other downstream network elements, is unavailable" and "monitor[] IP connections for transport alarms."[301] IP networks commonly do this by transmitting "heartbeat" signals at regular intervals between peer devices that trigger failover alarms automatically if heartbeats are not answered.[302]

Public safety commenters support this revised benchmark, which is substantively the same as proposed in the *NG911 Reliability FNPRM*.[303] They agree that a network monitoring requirement for IP-based CSPs is necessary and state that the Commission's proposal reflects the need for CSPs to quickly identify and address service disruptions.[304] Lumen acknowledges that the network monitoring requirement serves "to facilitate as soon as possible a provider's

---

[300] *CSRIC VI WG 1 Report* at 52.

[301] *Id.*; *2020 Best Practices Public Notice,* 35 FCC Rcd at 13179-81 (citing CSRIC best practice 12-9-0574). *See also* FCC, CSRIC Best Practices 13-10-0514 and 13-12-0608, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/about_data (last visited May 19, 2026) ("Network Operators [and] Service Providers should[,] when available, utilize a device management architecture that provides a single interface with access to alarms and monitoring information from all critical network elements;" "Network Operators [and] Service Providers . . . should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks (this includes OSPs and E9-1-1/NG9-1-1 SSPs)."). CSRIC best practices refer to both covered 911 service providers and OSPs as "service providers."

[302] *CSRIC VI WG 1 Report* at 52.

[303] The draft rule in Appendix A to the *NG911 Reliability FNPRM* stated that the monitoring requirement would apply to IP CSPs' covered facilities. *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2730. The Commission explained in the *NG911 Reliability FNPRM* that routing elements "responsible for path diversity" are critical facilities in the NG911 ecosystem that should be monitored. *See id.* at 2695-96, para. 68. We include IP routers, transport nodes, and node links used to meet the physical diversity requirement for covered 911 circuits and paths in the benchmark we adopt today for clarity.

[304] *See*, *e.g.*, COPUC Comments at 11 ("Both IP and legacy facilities should be monitored for disruptions continuously."); APCO Comments at 7.

response to, and notification to others regarding, an outage potentially affecting completion of 911 calls," but it argues the *NG911 Reliability FNPRM* proposal is overly prescriptive and that CSPs already employ robust network monitoring to comply with their outage notification duties under part 4 of the Commission's rules.[305] We do not believe the network monitoring benchmark is overly prescriptive, because it broadly describes functional capabilities—automatic disruption detection and alarming—without specifying a particular architectural solution or product. It therefore is consistent with the Commission's technology-neutral approach to facilitating reliability in NG911 networks.[306] We also disagree with the assertion that the revised monitoring benchmark is duplicative of the part 4 requirement to provide outage notification to PSAPs.[307] The PSAP outage notification rules do not include minimum network monitoring standards, and, moreover, do not apply to the new classes of CSPs identified in this order. In any event, CSPs with monitoring solutions in place can certify them as compliant with the benchmark or as alternative measures if necessary.

Other Benchmarks

Several commenters urge the Commission to add new reliability benchmarks addressing risks stemming from software failures, cyber attacks, and privacy breaches, and one initially endorsed the adoption of a "five nines" (99.999%) reliability standard. We agree that these are important considerations, but, at this time, we decline to adopt additional benchmarks beyond those proposed in the *NG911 Reliability FNPRM*.

Software diversity. NENA initially requested that the Commission add a software reliability benchmark to combat the rise of software defects as "the single most common cause of

---

[305] Lumen Comments at 8. *See also* 47 CFR § 4.9(h).

[306] *See*, *e.g.*, *NG911 Transition Order*, 39 FCC Rcd at 8159-60, paras. 39-40. *See also* APCO Comments at 7 (Network monitoring requirements should "allow for variances in CSP networks and implementation."). Nothing in today's *Order* prevents 911 Authorities or CSPs from exploring any available technology to monitor networks and detect and prevent outages. *See* Letter from Leo A. Wrobel, CEO, FailSafe Communications, Inc., to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 21-479, 13-75, at 2 (filed Jun. 10, 2026).

[307] Lumen Comments at 8 (arguing the "Commission's stringent Part 4 outage notification rules already entail robust network monitoring in order to comply with them.").

NG9-1-1 failure[.]"[308] It noted that, if components throughout a network are managed by the same software, then the software can act a single point of failure and disrupt service to an entire NG911 system.[309] NENA later withdrew its request, however, and asked the Commission to investigate software errors comprehensively in a different forum.[310] We agree that software failures have emerged as a cause of multi-state outages in recent years and that mitigating this threat is a priority.[311] The Commission recently re-chartered CSRIC and tasked it with investigating measures that will reduce common causes of "sunny day" outages, which include internal network failures due to software errors.[312] We defer consideration of this complex issue to a future proceeding, so we can develop a better record with contributions from all relevant stakeholders.

Cybersecurity. Several commenters suggest adding a reliability benchmark focused on defending against cyber threats.[313] Attempted cyberattacks against the nation's communications networks continue to be a major threat, and the Commission is taking steps to mitigate that threat through numerous rulemakings and enforcement actions.[314] We will continue to advance the implementation of cybersecurity measures in communications networks. We encourage NG911 service providers, OSPs, and 911 Authorities to support the cybersecurity of their systems during the transition to NG911, and we refer them to recommendations and best practices put forward by the Task Force on Optimal PSAP Architecture (TFOPA) and CSRIC VII. Both TFOPA and

---

[308] NENA Comments at 2, 21; Brian Rosen Reply at 3 ("We see more software defects as a root cause than any other source of failures in NG9-1-1 systems.").
[309] NENA Comments at 11; Brian Rosen Reply at 5-6 ("If every switch in an MPLS network is running the same software, or every switch in the underlying optical network runs the same software, then an ESInet that relies on that single network with the same software everywhere is not going to be reliable enough for 9-1-1.").
[310] NENA Reply at 3.
[311] *See 2014 Reliability NPRM*, 29 FCC Rcd at 14227, para. 45 (noting that the reliability and testing of software and databases used to process 911 calls, including planned maintenance and software upgrades, is an important area to address).
[312] *FCC Announces Intent to Re-Charter the Communications Safety, Reliability, and Interoperability Council and Solicits Nominations for Membership*, Public Notice, DA 26-134 (2026), https://docs.fcc.gov/public/attachments/DA-26-134A1.pdf.
[313] *See* Michigan State 911 Committee Comments at 1 ("The proposal would benefit from a more focus on cybersecurity. As NG911 becomes increasingly data-driven and interconnected, cyber threats pose a risk to service continuity. Resiliency must include cyber protections, guidance, and accountability."); Intrado Comments at 6; APCO Reply at 14.
[314] *See Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329, Order on Reconsideration, FCC 25-81, at 1-2, para. 1 & n.1 (Nov. 21, 2025) (summarizing initiatives).

CSRIC VII recommended adherence to the widely adopted approach to cyber defense detailed in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NCF).[315] CSRIC VII also recommended that 911 Authorities implement specific cybersecurity mitigation techniques, with, if necessary, the assistance of their NG911 vendors, including: continuous cyber monitoring, regular vulnerability assessments, minimum backups, a written cyber response plan, cyber-hygiene training, and other techniques.[316] Finally, we encourage NG911 service providers, OSPs, and 911 Authorities to leverage resources made available by other federal agencies, most notably CISA, to foster and enhance cybersecurity and to consider incorporating cybersecurity measures in their service agreements.[317]

Privacy protections. Public Knowledge supports our updated benchmarks, but it argues we should require CSPs to comply with consumer data privacy and other Customer Proprietary Network Information (CPNI) requirements when handling 911 traffic.[318] It identifies potential cyber breaches of customer data and carrier misconduct as risk vectors.[319] These risks are serious, but they are outside the scope of issues addressed in the *NG911 Reliability FNPRM*. We note as well that the Commission already prohibits carriers from making unwarranted disclosures of 911-related CPNI.[320] Because these rules protect the privacy of such information in both the legacy and the NG911 environment, we decline to adopt further privacy regulations in this proceeding.

---

[315] *TFOPA Scorecard* at 23-24; CSRIC VII, Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG 9-1-1 Implementations, § 6.2 (Sept. 16, 2020), https://www.fcc.gov/sites/default/files/csric7_report_secuirtyrisk-bestpracticesmitigationlegacytransitionalng911.pdf.

[316] CSRIC VII, Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and Next Generation 9-1-1 (NG911) Networks, § 5.2.1 (Mar. 10, 2021), https://www.fcc.gov/file/20607/download.

[317] *See*, *e.g.*, Cybersecurity & Infrastructure Security Agency, 911 Cybersecurity Resource Hub, https://www.cisa.gov/911-cybersecurity-resource-hub (last visited May 19, 2026).

[318] Public Knowledge Comments at 5.

[319] *Id.* at 6.

[320] *See, e.g.* 47 CFR § 64.2001 *et seq*. (implementing 47 U.S.C. § 222); *Location-Based Routing for Wireless 911 Calls*, PS Docket No. 18-64, Report and Order, 39 FCC Rcd 527, 562, para. 102 (2024); *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Fifth Report and Order and Fifth Further Notice of Proposed Rulemaking, 34 FCC Rcd 11592, 11614-16, paras. 49-52 (2019), *corrected by* Erratum (PSHSB Jan. 15, 2020). *See also* Lumen Reply at 8-9 ("Public Knowledge does not establish how safeguarding CPNI is a component of reliably completing 911 calls. Nor does [it] explain why the already-existing Commission requirement that telecommunications carriers and interconnected VoIP providers annually file with the Commission certifications confirming compliance with the CPNI rules does not suffice to promote Public Knowledge's objectives.").

"Five Nines" Reliability. The Commission asked in the *NG911 Reliability FNPRM* whether it should incorporate a "five nines" metric into the 911 reliability framework, referring to a measure of reliability equal to 99.999% network availability, which allows only 5.26 minutes of downtime in a year.[321] NENA initially indicated its support and observed that five nines already is a service level requirement in many contracts between 911 Authorities and their NGCS vendors.[322] However, NENA also indicated that NGCS providers often cannot achieve this standard; that determining a reliability metric across an NG911 network would require CSPs to share proprietary network information and to retain outside experts; and that there could be disagreements over which types of outages qualify as failures of reliability and how to calculate the metric.[323] NENA later withdrew its support and now advises that a five nines requirement for CSPs "warrant[s] significant further investigation."[324] We are persuaded by NENA's comments and by the overall lack of support in the record that it is premature to introduce a five nines requirement at this time. However, we strongly support the efforts of 911 Authorities to increase the reliability of their NG911 networks by negotiating rigorous service level agreements with NG911 CSPs, and we encourage other CSPs to adopt the five nines standard as an internal target to guide ongoing network performance improvements.

Interoperability

Today, we adopt a definition of interoperability and require NGCS and ESInet CSPs to submit a one-time report describing the actions they have taken, and plan to take, to implement interoperability. These measures will support the ongoing work of 911 Authorities and their industry partners as they strive toward implementing seamlessly interoperable NG911 systems.

---

[321] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2692-93, para. 61 (citing *In the Matter of the Nebraska Public Service Commission, on its own motion, conducting an investigation into the 911 service outage that began on August 31, 2023 in areas of Nebraska served by Lumen*, Application Nos. 911-075/PI-248 and 911-077/C-5581/PI-252, Order Issuing Findings and Closing Investigation at 24 (Jan. 15, 2025), https://www.nebraska.gov/psc/orders/state911/2025-01-14%20911-075%20PI-248%20911-077%20C-5581%20PI-252%20Order%20Issuing%20Findings%20and%20Closing%20Investigation.pdf (*Nebraska PSC Order*).

[322] NENA Comments at 17.

[323] NENA Comments at 17-19; Brian Rosen Reply at 8 ("Virtually all such contracts have 5 nines [service level agreements], but we have seen many multi-hour failures."). *See also Nebraska PSC Order* at 24 (summarizing testimony from Brian Rosen describing "two ways to determine availability").

[324] NENA Reply at 4.

It is essential that NG911 networks enable the seamless transfer of 911 calls and data. The ability to reliably share, transfer, and validate location data is not just a feature of NG9-1-1; it is its foundation.[325] That is why the Commission defined NG911 as a system that ensures interoperability and supports the sharing of information related to 911 requests for emergency assistance among emergency communications centers and emergency response providers.[326] Interoperable NG911 systems strengthen the resiliency and reliability of NG911 services not just during natural disasters, outages, and large-scale events,[327] but also in the provision of mutual aid and ensuring fast and efficient handling of 911 calls and data.[328] Interoperability between NG911 systems and providers is a key component of the "end state" envisioned by TFOPA when it defined the stages of the transition to NG911 service.[329]

Based on the record, we find that it is premature to adopt substantive interoperability standards and testing requirements at this time. In the accompanying *Second Further Notice*, we seek comment on additional proposals to promote greater interoperability across NG911 systems.

Interoperability Definition

Defining interoperability is necessary to precisely identify the specific operational issues that we intend to address in this proceeding. The definition we adopt today is one that envisions a NG911 ecosystem where 911 Authorities can seamlessly receive, process, and share

---

[325] Victoria Ogaga, *The Hidden Crisis: Why Location Data Fails in Emergency Responses*, (Mar. 24, 2026), https://www.intrado.com/blog/blog-location-data-and-call-handling-solutions?utm_campaign=37974662-CC%20-%20VNG&utm_medium=email&_hsenc=p2ANqtz-8YdQ1o6yAma1ZpVlZ9eArjE6Nw3pti-FFOMEjVjjpUSLYZx011UFemZeFxiMx8qL1NAPq926ZB3LNQ1yLJR3i00qs76Q&_hsmi=411564505&utm_content=411564505&utm_source=hs_automation.

[326] 47 CFR § 9.28; *NG911 Transition Order*, 39 FCC Rcd at 8160, para. 39 ("In particular, the definition adopted today . . . contains the important requirements that an NG911 system ensure interoperability, be secure, and employ commonly accepted standards.").

[327] NC 911 Board, Hurricane Helene, September 2024 at 11, https://content.govdelivery.com/attachments/NC911BOARD/2026/04/01/file_attachments/3604052/NC911%20Board%20Hurricane%20Helene%20After%20Action%20Report%202025.08.18_FINAL.pdf.

[328] Sam Gaither comments on behalf of the South Carolina Coastal Area Cooperative (SCCAC), at 1; City of Coconut Creek, FL July 21, 2025 Comments at 1; NENA Comments at 8.

[329] *See TFOPA Scorecard, passim*. The TFOPA activity defined states of transition ranged from today's legacy state, through foundational, transitional, and intermediate states, culminating in the jurisdictional and nation-wide "end states" of NG911 service. Per TFOPA, "End State" refers to the state in which PSAPs have evolved to become ECCs and are served by standards-based NG911 systems and/or elements and OSPs are providing SIP interfaces with location information during call setup, and ESInets are interconnected providing interoperability on a national basis, supported by established agreements, policies and procedures.

emergency requests across different jurisdictions, technologies, devices, and systems. In the *NG911 Reliability FNPRM,* the Commission sought comment on whether a definition of "interoperability" was needed in order to clarify the obligations of NG911 service providers.[330] Specifically, the Commission sought comment on whether the definition of "interoperability" from the Spectrum Auction Reauthorization Act of 2023 (H.R. 3656)[331] would help to define the scope of any future interoperability requirements.[332]

Commenters generally support adopting an interoperability definition that tracks language in proposed legislation, with minor variations. APCO states that "the public safety community has developed a definition of interoperability that reflects its operational needs and that has been incorporated into legislative proposals," and urges the Commission to adopt this definition.[333] ATIS urges the Commission to adopt a formal definition of "interoperability" in the context of NG911.[334] NENA advocates using the definition included in H.R. 1784 - Next Generation 9–1–1 Act of 2023,[335] while T-Mobile proposes a definition that is similar to the two proposed legislative definitions.[336]

Given the relatively slight differences between the various proposed definitions, we adopt the following definition that aligns with the consensus reflected in H.R. 3565 and is designed to promote interoperability and discourage proprietary features:

> The technical and operational capability of NG911 service providers to exchange 911 voice, text, data, and multimedia between jurisdictions, PSAPs, ECCs, and other service

---

[330] *NG911 Reliability FNPRM,* 40 FCC Rcd at 2699, para. 80.

[331] H.R. 3565 defines the term "interoperability" as

> the capability of emergency communications centers to receive 9–1–1 requests for emergency assistance and information and data related to such requests, such as location information and callback numbers from a person initiating the request, then process and share the 9–1–1 requests for emergency assistance and information and data related to such requests with other emergency communications centers and emergency response providers without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.

H.R. 3565, § 301.

[332] *NG911 Reliability FNPRM,* 40 FCC Rcd at 2699, para. 80.

[333] APCO Comments at 3; see also APCO Reply at 9.

[334] ATIS Reply at 6.

[335] NENA Reply at 7.

[336] T-Mobile Reply at 5.

providers, in real time without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.[337]

This definition, while substantially similar to the H.R. 3565 definition, is intended to encompass the entire call flow from initiation through resolution while remaining technologically neutral. Technological neutrality is important to ensure this definition remains relevant as the technological capabilities of NG911 expand and evolve. We also add "NG911 service providers" to the definition of interoperability in acknowledgement of the technical limitations of legacy 911 systems and to signal our intent to apply interoperability requirements only to NG911 systems.

One-Time Reporting Requirement

We require NGCS and ESInet providers, which have a direct role in enabling interoperability as defined in this *Order*, to submit a one-time report to the Commission describing the specific actions they have taken, as well as their plans for future actions, to enable NG911 interoperability consistent with that definition.[338] We allow 18 months to submit this report to provide CSPs adequate time to assess their interoperability capabilities, document existing interoperability arrangements, and prepare accurate reports.[339] This reporting requirement is intended to encourage these entities to prioritize and accelerate their interoperability efforts, while providing the Commission with a greater understanding of the overall progress of interoperability across the entire NG911 ecosystem. We believe these reports will promote continued focus on interoperability issues as part of the NG911 transition and will provide us with important information on whether any additional interoperability requirements are needed to advance the transition.[340]

---

[337] Appendix A (§ 9.19(a)(19)).
[338] *See* Appendix A (§ 9.20(b)).
[339] Entities that begin providing covered 911 services after the interoperability reporting deadline must submit a one-time interoperability report when they begin providing services.
[340] iCERT Comments at 16; iCERT Reply at 8-9.

Commenters note that facilities interconnecting ESInets are only one type of facility needed to ensure interoperability for interstate 911 live call transfers across multiple touchpoints in NG911 systems (e.g., ESInet to ESInet, NGCS to NGCS, PSAP to PSAP).[341] We agree that achieving full interstate NG911 interoperability will require more than ESInet-to-ESInet interoperability alone. Nevertheless, given that this is the first time the Commission has adopted 911 interoperability measures, and in order to maximize public interest benefit impact with the least amount of regulatory burden, we are limiting the applicability of the reporting requirement to NGCS and ESInet providers. These entities supply critical call routing and transfer services that enable the connection between an NG911 call initiator and an NG911 PSAP. We believe focusing on these providers is not only a significant step forward towards increased interstate interoperability; we also anticipate that this step will incentivize the further development of interoperability solutions in other aspects of the NG911 ecosystem, including local and intrastate interoperability.[342]

Interoperability Benchmarks and Testing

Benchmarks. We decline, in this *Order*, to mandate specific interoperability benchmarks or testing requirements. In the *NG911 Reliability FNPRM*, we proposed to require that CSPs certify whether their interstate interconnecting ESInet facilities achieve interoperability for exchanged 911 traffic sufficiently to enable complete interstate transfers between ESInets or certify to alternative measures.[343] However, there was considerable disagreement in the record with regards to the need for, efficacy of, and scope of our proposed interoperability certification requirements.[344] Commenters generally agree that interoperability is critical to the success of

---

[341] *See e.g.* NENA Comments at 9, 12; NASNA Comments at 7; APCO Comments at 3.
[342] NENA Reply at 7; Texas 9-1-1 Entities Comments at 4.
[343] *NG911 Reliability FNPRM,* 40 FCC Rcd at 2697, para. 72. We proposed requiring CSPs to certify whether their NGCS and/or ESInet facilities use conformance-tested equipment and whether they have tested their interstate interoperability capabilities. We further proposed allowing CSP to certify in the alternative: (1) whether it (or its ESInet facility operator) has taken alternative measures to ensure interoperability between ESInets in multiple states and between providers; (2) whether it believes that one or more of the requirements of this paragraph are not applicable to its facilities; and (3) to additional questions about the non-conforming facilities as directed by the Bureau. *Id*.
[344] Lumen Comments at 2, 10-11; Motorola Comments at 2; NENA Comments at 6-7; Verizon Reply at 3-4; CTIA Reply at 8-9; NENA Reply at 3.

NG911 but disagree on the timing of regulatory action and whether industry-led standards development could supplant the need for Commission action. Industry commenters and standards bodies argue that the Commission should either delay establishing a requirement pending further study or defer establishing a requirement altogether and allow interoperability solutions to evolve as a natural result of market forces.[345] Public safety commenters urge the Commission to act now as delay will only embed existing incompatibilities.[346]

Collectively, the record reflects that 911 Authorities and CSPs have begun to take steps to enable interoperability between NG911 systems, but that this work is still in its very early stages.[347] Demonstrated interoperability sufficient to permit policy routing and seamless transfer of NG911 traffic across jurisdictional boundaries is still the exception rather than the norm, and capabilities to enable cross-jurisdictional dispatch are even more rare.[348] Given that this subject remains unsettled, we decline to adopt interoperability standards at this time.

Testing. The Commission proposed in the *NG911 Reliability FNPRM* to require CSPs to certify whether their interstate interconnecting ESInet facilities use conformance-tested equipment and whether they have tested their interstate interoperability capabilities.[349] The record reflects support in principle for conformance and interoperability testing,[350] but commenters express concern that the current lack of specificity on significant components of conformance and interoperability testing would hinder implementation of a robust and effective

---

[345] *See* Intrado Comments at 25; iCERT Comments at 16; T-Mobile Comments at 7-8; CTIA Reply at 8-9; NENA Reply at 2-3; ATIS Comments at 3-4; DATAMARK Reply at 8.
[346] *See* APCO Reply at 8; Michigan State 911 Committee Comments at 1; CCOA Reply at 3; Texas 9-1-1 Entities Comments at 3-4.
[347] *See*, *e.g.*, BRETSA Reply at 15-16 ("Different states are at different stages in deploying ESInets, implementing and migrating to i3 NG9-1-1 service, and of readiness for interconnecting their 9-1-1 networks with those of adjacent states.").
[348] Donny Jackson, *Motorola Solutions touts ESInet interop with AT&T in Maryland* (Dec. 10, 2025), https://urgentcomm.com/interoperability/motorola-solutions-touts-esinet-interop-with-at-t-in-maryland; North Carolina Department of Information Technology, *North Carolina and Washington, D.C., Partner to Demonstrate Nation-Leading Next Generation 911 Resiliency* (Feb. 12, 2026), https://it.nc.gov/news/press-releases/2026/02/12/north-carolina-and-washington-dc-partner-demonstrate-nation-leading-next-generation-911-resiliency; Fairfax County, *County 9-1-1 Launches First Interstate Backup System in the United States* (Feb. 6, 2025), https://www.fairfaxcounty.gov/news/county-9-1-1-launches-first-interstate-backup-system-united-states.
[349] *NG911 Reliability FNPRM,* 40 FCC Rcd at 2697, para. 72.
[350] APCO Comments at 4; SCCAC Comments at 2; 1Spatial Comments at 4.

testing regime.[351] Commenters cite the relative immaturity of the testing ecosystem, lack of testing entities and facilities, standardized procedures, and the identification of a commonly accepted standard.[352]

Given the lack of foundation in the record that would be needed to establish a meaningful testing regime, we find it neither prudent nor productive to impose testing or associated certification requirements at this time. However, in order to facilitate reporting and inform future work on NG911 interoperability, we adopt definitions of "interoperability standards testing" and "interoperability conformance testing." In the companion *Second Further Notice*, we seek comment on further steps to promote interoperability, including empowering our state partners to develop mechanisms enabling them to craft the level of interoperability that they believe appropriate to their state.[353]

Oversight

As proposed in the in the *NG911 Reliability FNPRM*, we adopt targeted updates to strengthen the oversight of 911 reliability and interoperability by the Commission and by 911 Authorities while lessening compliance burdens on CSPs.[354] First, we replace annual reliability certifications with a one-time initial certification and a continuing obligation to update that certification following any material change. We also direct the Bureau to streamline the form that CSPs will use to submit their reliability certifications and to update it to reflect the changes to the 911 reliability framework we adopt today. Second, we grant state, territorial, and tribal 911 Authorities access to CSPs' reliability certifications and interoperability reports, conditioned on their adherence to robust confidentiality safeguards. And third, to provide transparency to CSPs, we codify the administrative process the Bureau will follow in the event it becomes necessary to remediate a CSP's noncompliance with its 911 reliability obligations. We decline

---

[351] Brian Rosen Reply at 3-4.
[352] ATIS Reply at 4-5; A2LA Comments at 1; Motorola Reply at 3-4; 1Spatial Comments at 4-5; NENA Comments at 7, 13-14; Brian Rosen Reply at 3-5; Motorola Comments at 5; ATIS Comments at 5; 1Spatial Comments at 4-5; NASNA Comments at 8-9.
[353] *See* DATAMARK Reply at 8; BRETSA Reply at ii.
[354] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2702-2710, paras. 88-110.

to adopt several oversight proposals from the *FNPRM*, including the creation of a new portal for consumer complaints and a petition process for 911 Authorities, because we find them to be unwarranted at this time.

Reliability Certification Process

We update the reliability certification process to ensure continued CSP accountability while reducing regulatory burdens. First, we eliminate the requirement for CSPs to file reliability certifications annually. We conclude that annual filing is not an effective means of obtaining timely and actionable information regarding network reliability and that it results in needless annual reporting burdens for CSPs when there may be no material changes to their networks or reliability practices from year to year. Going forward, CSPs will only be required to submit an initial compliance certification and to update it in the event of a material change to the information covered by the certification.

Second, we eliminate the requirement for certifications to separately document reliability practices with respect to each individual PSAP served by the CSP. While this level of detail may have been appropriate for ensuring reliable connectivity between legacy selective routers and TDM-based PSAPs, IP-based CSPs typically implement reliability measures at the network or service-platform level. For example, where an ESInet provider incorporates physical diversity and enables dynamic rerouting of calls among multiple PSAPs, requiring reliability certifications on a per-PSAP level yields little unique information while imposing significant administrative burdens. We therefore allow CSPs to file consolidated certifications for their facilities at the network level, provided that facilities serving multiple states are identified on a per-state basis to facilitate evaluation by 911 Authorities.

Third, the updated certification process provides relief for IP-based CSPs that previously certified to common IP reliability practices as "alternative measures," which required them to include narrative explanations and justifications in their certifications. These measures are now specifically identified as best practices that meet the reliability benchmarks of the updated rules.

Accordingly, CSPs may certify to their use without the need for lengthy narrative explanations or other burdensome filing requirements.

Going forward, under the updated certification process we adopt today, CSPs will submit a one-time certification addressing the three elements of reliability (physical diversity, operational integrity, and network monitoring) and, thereafter, file updated certifications only on an as-needed basis. To provide time for compliance with the new reliability benchmarks, CSPs will not need to file the initial certification until 18 months after a public notice announcing a compliance date.[355] CSPs must also update their certifications within 90 days of discovery of any material change to their ownership structure, networks, facilities, operations, or reliability practices that renders the prior certification inaccurate or incomplete. This approach minimizes the burden on providers while ensuring that the Commission has the benefit of an accurate, up-to-date record of the reliability practices that are protecting 911 connectivity.[356] We emphasize that the purpose of the certification requirement is to ensure that the Commission and relevant 911 Authorities have accurate and current information regarding CSP reliability practices. Therefore, CSPs are responsible for exercising reasonable judgment in determining whether a change is material and ensuring that their certifications are complete, accurate, and up to date at all times.[357]

We agree with USTelecom that "material changes" should exclude changes remedied within 90 days of discovery and *pro forma* ownership changes, and that carriers should exercise reasonable judgment about when an update is required.[358] We also agree with USTelecom that frequent updates for network improvements would be burdensome to CSPs and not helpful for

---

[355] Entities that begin providing covered 911 services after that initial certification compliance date must submit an initial reliability certification when they begin providing services.

[356] *See* NENA Comments at 19 (encouraging the Commission to "simplify reporting requirements" while maintaining "a complete picture of what happened, and any corrective actions to be taken").

[357] As under the previous rules, certifications must be signed by an official under penalty of perjury as to the accuracy of their contents. *See* Appendix A (§ 9.19(a)(2)).

[358] Letter from Nirali Patel, Senior Vice President, Regulatory & Legal Affairs and General Counsel, USTelecom, to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 21-479, 13-75, at 2-3 (filed Jun. 18, 2026).

oversight,[359] and we therefore exclude improvements for less than 50 percent of a CSP's covered 911 services, circuits, and paths. This will eliminate excessive filings while preserving reasonable awareness of major network reliability improvements. CSPs are free to file more frequent updates for lower threshold improvements, either on their own or upon agreement with a 911 Authority, including targeted updates for improvements limited to specific states or regions.

We also require CSPs covered by the updated rules that have not previously filed a reliability certification to file an attestation identifying themselves as covered 911 service providers.[360] Attestations will be due six months after the Bureau issues a public notice announcing the commencement of the 18-month transition period for coming into compliance with the updated reliability rules. The attestations will enable the Commission and 911 Authorities to identify the scope and number of CSPs participating in the NG911 ecosystem before CSPs submit their initial reliability certifications.

Consistent with the *NG911 Reliability FNPRM*, we direct the Bureau to revise the reliability certification process to incorporate our revisions to the 911 reliability framework and to make general improvements to the form.[361] We delegate authority to the Bureau to make such changes to the form as are needed to streamline the process for providers and to collect data in formats that will allow Bureau staff to easily sort and analyze it.[362] We also direct the Bureau to implement streamlined filing requirements by revising the instructions to facilitate certifications consistent with today's framework, and with the goal of reducing compliance burdens on regulated entities.

---

[359] *Id*. at 3.
[360] *See* Appendix A (§ 9.19(a)(1)).
[361] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2702-04, paras. 90-92.
[362] *Id.* at 2704, para. 92; *Public Safety and Homeland Security Bureau Seeks Comment on Modifications to Network Outage Reporting system and 911 Reliability Certification System*, PS Docket Nos. 15-80, 13-75, Public Notice, 35 FCC Rcd 4409, 4413 (seeking comment on adding "drop-down fields to 911 reliability certifications that will require covered 911 service providers to indicate whether they provide" specified 911, E911, or NG911 services) (PSHSB 2020). We entrust to the Bureau's judgment how to best streamline the form while retaining options for longform narrative explanations where necessary.

Reporting 911 call volume. At this time, we do not require CSPs to report the volume of 911 call traffic that their non-conforming facilities handle.[363] The Commission proposed this addition in response to previous comments from state government entities in other proceedings.[364] While information regarding CSPs' 911 call volumes could be beneficial to enable the Bureau to better identify and address areas that are exposed to outsized risk of major disruptions to 911 service,[365] the record shows that collecting this data may be technologically infeasible for some CSPs at this time or would require significant cooperation from vendors and PSAPs.[366]

Certification regarding leased facilities. Several industry commenters urge the Commission to limit NG911 CSPs' certification responsibility to the network elements they operate themselves and to exclude the transport paths and functional elements they lease from third parties. These commenters claim that their third-party providers have too much market power and refuse to share information with them about their networks' path diversity.[367] APCO, on the other hand, argues that CSPs "must be accountable for the actions of their third-party contractors, including the measures those parties take to maintain reliability," and NENA supports this view.[368]

The Commission's longstanding practice has been to require CSPs that lease transport or other facilities to certify how they meet their reliability obligation through their leased

---

[363] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2705, para. 94.
[364] *See*, *e.g.*, NASNA Comments, PS Docket 13-75, at 3 (filed July 17, 2020) (recommending changes to the reliability certification form to "allow the FCC to analyze filed Reliability Certification Systems to know what populations are being made vulnerable to outages due to lack of redundancy or diversity in 911 networks); *see also* Colorado Public Utility Commission Comments, PS Docket 13-75, at 2 (filed July 8, 2020).
[365] *Cf.* Lumen Comments at 9-10 (arguing that "there is no nexus between the proposed data point and the Commission's oversight of 911 reliability," yet also acknowledging that 911 call volume would "be a data point for the Commission to consider in attempting to predict the impact of a 911 outage associated with facilities not adhering to the Commission's 911 reliability requirements"); 47 CFR § 0.392.
[366] *See*, *e.g.*, Brian Rosen Reply at 10 (observing that it is "not feasible" to collect 911 call volume data from IP networks "because the routers that have the raw data don't know what the contents of the IP packets they are handling is"; noting further that 911 Authorities would need to compel their vendors to make logging data available for other CSPs to comply); Lumen Comments at 9 ("[A]massing this data entails inputs from numerous PSAPs and subcontractors, not all of whom are prone to respond with alacrity.").
[367] Comtech Comments at 8 ("CSPs should only be required to certify reliability measures that are within their operational control . . . ."); iCERT Comments at 13; Intrado Reply at 6.
[368] APCO Reply at 15; *see also* NENA Comments at 12-13 (arguing that a 911 Authority's NGCS vendor should be responsible for certifying the reliability of its subcontractors' facilities).

facilities.[369] We see no basis to change this practice. Our updated designation of key NG911 service providers as CSPs in today's *Order* will provide additional transparency with respect to their reliability practices. We expect OSPs, CSPs, 911 Authorities, and their vendors to collaborate as needed to facilitate compliance with our 911 reliability framework and to support a strong, resilient, and interoperable NG911 ecosystem. With respect to certification, CSPs that lease or otherwise rely on third-party facilities should certify to network practices within their control and may cite to representations provided by third parties in service level agreements. In cases where a CSP cannot obtain necessary information from a third party it uses to provide NG911 service, the CSP should describe in its certification the efforts it made to obtain the information and why those efforts were unsuccessful. The Commission will take these circumstances into consideration when evaluating the sufficiency of the CSP's certification.[370]

Other changes to the certification process. We do not find sufficient support in the record to change the certification process in other ways that some commenters suggest.[371] Home Telephone, for example, advocates requiring ESInet operators to prove their financial, technical, and managerial resources and receive advance certification from the Commission before they may provide services to 911 Authorities.[372] We decline to take this step because 911 Authorities have the ability to require such disclosures when soliciting bids from potential ESInet providers, and, as Lumen observes, "the record contains no allegations[] of ESInet providers [being] chronically unprepared to provide service successfully."[373] We also see no need, at this time, to

---

[369] *911 Reliability Order*, 28 FCC Rcd at 17506, para. 90 ("Although it could contract with the underlying facilities lessor, if necessary, to audit its facilities, the [CSP] would remain responsible under our rules for ensuring compliance with the auditing requirement."); *2015 911 Reliability Recon. Order*, 30 FCC Rcd at 8657, para. 17 ("[T]he contracting out of certain functions . . . does not absolve individual [CSPs] of their respective obligations for reliable 911 service."). *See also* 47 U.S.C. § 217 ("[T]he act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person.").
[370] Because each CSP will certify the reliability of its own facilities and any subcontracted or leased facilities it uses to provide 911 service, we find that there is no cause for CSPs to submit a "chain-of-responsibility matrix" on behalf of their subcontractors, as two commenters proposed. *See* CCOA Comments at 4; Lumen Reply at 7-8.
[371] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2706, para. 97 (soliciting suggested measures that would promote 911 reliability and interoperability in addition to certifications).
[372] Home Telephone Comments at 9.
[373] Lumen Reply at 8.

require CSPs to submit to periodic third-party testing and audits to confirm the accuracy of their reliability certifications.[374] While we encourage CSPs to perform periodic testing and auditing, and while 911 Authorities have discretion to include testing and auditing provisions in their contracts with CSPs, requiring such measures by rule could greatly increase the cost of compliance and we prefer to permit flexibility for any testing and auditing measures that support accurate reliability certifications.

Simplifying regulatory language. We adopt minor amendments to the regulatory text implementing our 911 reliability framework to improve clarity and thereby reduce compliance burdens on covered entities.[375] Specifically, we consolidate the certification and other filing requirements that formerly appeared across former §§ 9.19(c)(1) through 9.19(c)((3) and move them to a new § 9.20, entitled "Reliability and Interoperability Certifications; Cessation Notices." This change simplifies § 9.19, which now relates solely to CSPs' substantive obligations to provide reliable 911 services. Section 9.20 now addresses procedural matters associated with the reliability requirement, including certifications, confidentiality, record retention, cessation notices, and remedial actions. We also have made non-substantive, streamlining changes to certain regulatory language, including to the record retention subparagraphs under former § 9.19(d)(3), as proposed.[376]

911 Authority Access to Certifications and Reports

We adopt, with some modifications, the Commission's proposal to ensure that 911 Authorities can access CSP reliability certifications and interoperability reports.[377] The Commission has long recognized that 911 Authorities should have access to CSPs' submissions to inform their planning and oversight of the 911 networks serving their jurisdictions. When the

[374] CCOA Reply at 7 ("CCOA strongly encourages that the rules require periodic testing and sporadic auditing by someone external to the carrier to verify that the content of the CSP's annual certification is accurate and reliable."); 1Spatial Comments at 3 ("Any NG911 interoperability certification must include a component that verifies the data[.]").
[375] *See* Appendix A (§§ 9.19, 9.20); *NG911 Reliability FNPRM*, 40 FCC Rcd at 2706, para. 96.
[376] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2706, para. 96.
[377] *Id.* at 2706-08, paras. 98-103; Appendix A (§ 9.20(c)-(d)).

Commission adopted the 2013 reliability rules, it recognized that PSAPs and 911 Authorities "have a strong interest in obtaining relevant information about the reliability and resiliency of their 911 service" and might need additional information "to prompt [CSPs] to make specific reliability improvements in their networks."[378] The Commission did not mandate disclosure to PSAPs or 911 Authorities at that time "[i]n light of the wide variety of circumstances involved in how PSAPs nationwide purchase 911 service," but it admonished CSPs to "respond promptly" to disclosure requests and to "enter into discussions concerning the content of the provider's 911 circuit auditing certification."[379] The Commission concluded "that PSAPs should have access to the details of circuit-auditing certifications, as long as the sensitive and proprietary nature of the information can be maintained."[380]

The record in this proceeding indicates that disclosure of CSP reliability certifications and interoperability reports is more critical today than in 2013, because the NG911 ecosystem now involves a wider array of providers, traffic aggregators, and subcontracted facilities that may not have direct relationships with the PSAPs and 911 Authorities whose 911 traffic they process and carry. The increasingly diffuse nature of the NG911 ecosystem makes it more difficult for 911 Authorities to fully assess the reliability and interoperability of their 911 services without access to provider network information, especially from distant CSPs that provide NG911 capabilities on the OSP side of the NG911 ecosystem.[381]

Public safety and industry commenters broadly agree that 911 Authorities should be entitled to access CSP submissions, subject to confidentiality protections.[382] Commenters note that "[t]he 911 community is currently lacking access in this area and [that] having access to

---

[378] *911 Reliability Order*, 28 FCC Rcd at 17532-33, paras. 156-57.
[379] *Id.* at 17533, para. 157-58 ("The record in this proceeding supports allowing PSAPs and, as relevant, state 911 authorities, access to potentially sensitive information on the circuit routes to the PSAP.").
[380] *Id.* at 17533, para. 158.
[381] *Massachusetts Ex Parte* at 4-5 (identifying need for 911 Authority visibility and oversight into third-party 911 service providers to OSPs based on Massachusetts' experiences during the NG911 transition).
[382] *See*, *e.g.*, CCOA Comments at 3 ("We recommend that the final rule grant 911 Authorities the right to obtain, review, and validate CSP certifications and documentation, including alternate reliability measures and identified single points of failure."); Michigan State 911 Committee Comments at 1 ("This transparency would improve oversight and allow us to identify vulnerabilities early, instead of after outages have already occurred.").

information about covered service providers' certifications would be extremely useful. Knowledge of the points of vulnerability in the 911 network serving a state or an individual PSAP will help state and local 911 officials better plan for and mitigate the risks of outages and disruptions."[383] CCOA agrees that "[f]or their advance operational planning, 911 Authorities must be able to rely on the CSP's identification of where critical 911 circuits are diverse and where they are not."[384] Lumen notes that the Commission's proposal is "undergirded by appropriate safeguards and already-existing processes" and is cabined appropriately to government entities "with a need-to-know basis."[385]

Given the strong and consistent responses of most commenters, we are not persuaded by Verizon's dissenting view that 911 Authorities do not want or need access to 911RCS filings.[386] Nor do we agree that CSPs should be permitted to redact descriptions of their alternative measures and other "specific technical details," as one commenter suggests.[387] That is precisely the type of information 911 Authorities need to identify potential single points of failure and other vulnerabilities, and we believe the confidentiality and redaction protections we adopt today are sufficient to avoid unnecessary disclosures of network information. As one provider puts it: "As we evolve our 911 system into the NG911 environment[,] . . . local PSAPs lose visibility into the reliability of many of the elements required for the functioning of the system. Importantly[,] our local PSAPs and even our State 911 Authorities lose visibility in the operations of national NG911 ESInet aggregators as well as national transport providers."[388] In

---

[383] NASNA Comments at 6-7; *see also*, *e.g.*, CCOA Comments at 3; Michigan State 911 Committee Comments at 1 ("This transparency would improve oversight and allow us to identify vulnerabilities early, instead of after outages have already occurred."); NYSPSC Comments at 2 ("As with NORS access, expanding transparency to these certifications will enable state and local 911 authorities to more accurately assess and identify how 911 providers and PSAPs interact within the state along with existing limitations in the NG911 environment exist."); COPUC Comments at 11-12; Intrado Comments at 22-23.
[384] CCOA Reply at 6-7.
[385] Lumen Comments at 12-14.
[386] Verizon Comments at 16 ("To date there has been very little demand by state and local government 911 authorities for wireline 911 providers' annual certifications[.]"). Verizon's observation, if true, could be due to 911 Authorities' focus in recent years on transitioning away from legacy wireline 911 services to NG911. These efforts underscore the need for 911 Authorities to have access to the certifications of IP-based CSPs.
[387] Intrado Comments at 23.
[388] Home Telephone Comments at 13.

this more complex environment, we find that voluntary disclosure is no longer sufficient to ensure that 911 Authorities consistently receive all of the information they need to safeguard the reliability of the 911 systems they oversee.[389]

Separately, we conclude that providing 911 Authorities with access to CSP reliability and interoperability filings will amplify the Commission's ability to address potential risks to NG911 service and possible violations of the Commission's 911 reliability framework.[390] Although the Commission is ultimately responsible for enforcement of its framework, 911 Authorities have a shared interest in protecting the reliability of NG911 networks, and we believe their oversight will complement our own. 911 Authorities are better positioned than the Commission, in some cases, to identify compliance issues, because they are customers of NG911 services and regularly coordinate with CSPs regarding service problems. Enabling 911 Authorities to report concerns to the Bureau therefore will improve the Commission's oversight while conserving Bureau resources and freeing staff to focus their attention on critical risks that could result in multistate and multi-OSP outages or hamper interstate interoperability.

Confidentiality protections. As proposed in the *NG911 Reliability FNPRM*, we retain the presumption of confidentiality for proprietary information in reliability certifications, and we require 911 Authorities seeking access to CSP reliability certifications and interoperability reports to comply with the same confidentiality safeguards that protect NORS outage reports when state agencies are given access to them.[391] The Commission allows state, territorial, and tribal agencies to access NORS reports on a need-to-know basis, conditioned on their agreement

---

[389] We acknowledge that some 911 Authorities may already receive state reliability certifications from certain 911 service providers operating within in their jurisdictions. Even in such cases, 911 Authorities can use FCC reliability certifications and interoperability reports to verify the local submissions. COPUC Comments at 11-12.

[390] *See*, *e.g.*, NYSPSC Comments at 2 ("[T]he availability of this information will also better position state and local 911 authorities to offer more substantive and effective recommendations to the FCC in future NG911 proceedings."); *see also* Washington Utilities and Transportation Commission Comments, PS Docket No. 14-193 at 8 (filed March 17, 2015) ("Access to such information by state officials would greatly assist in understanding and tracking marketplace developments affecting 911 service delivery within the scope of their jurisdictions. State access could also greatly assist officials during times of emergency . . . in understanding and interacting with such entities as events unfold.").

[391] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2708, para. 101; 47 CFR § 9.19(d)(2)(i), (ii) (confidentiality of 911RCS certifications).

to robust confidentiality protections.[392] The NORS protections are set forth in their entirety through the codified provisions in §4.2 of part 4 of the Commission's rules and the guidance, instructions, and forms the Bureau has published on the Commission's website.[393]

We find that the NORS data protections are an appropriate and effective model for safeguarding reliability certifications and interoperability reports. The NORS framework reflects a mature, field-tested set of safeguards that already balances state and tribal agencies' need for operationally meaningful network information with the imperative to protect service providers' proprietary data. Aligning the confidentiality obligations for NORS reports and reliability certifications and interoperability reports likewise reduces administrative uncertainty for both agencies and providers, promotes consistent treatment of sensitive reliability information across Commission programs, and preserves strong incentives for CSPs to participate fully and candidly in the certification process.

Accordingly, we permit CSPs to condition their production of reliability certifications and interoperability reports to 911 Authorities on their execution of confidentiality agreements with terms that are not more restrictive than those set forth in § 4.2 and the Bureau's supplemental guidance.[394] We also clarify that only statewide, territorial, and tribal 911 Authorities may request copies of CSPs' certifications and reports. While we recognize that allowing local or regional 911 Authorities to access CSP certifications and reports could also be beneficial in some instances—particularly in home rule states where such entities have responsibilities for NG911 planning and deployment decisions—we find that extending access to potentially hundreds of government entities would impose undue burdens on CSPs and could result in an unwarranted

---

[392] *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications,* PS Docket No. 15-80, Second Report and Order, 36 FCC Rcd 6136, 6137, para. 3 (2021) (*NORS Information Sharing Order*). See also id. at 6143-97, paras. 22-128 (summarizing confidentiality protections).

[393] *See* 47 CFR § 4.2; FCC, Outage Information Sharing, https://www.fcc.gov/outage-information-sharing (last visited May 19, 2026) (including the posted documents "How to Apply for Access," "Participating Agency Certification Form," and "Downstream Agency Certification Form"). *See also NORS Information Sharing Order*, 36 FCC Rcd at 6143-97, paras. 22-128 (explaining the NORS access rules and procedures).

[394] *See* FCC, *Outage Information Sharing*, https://www.fcc.gov/outage-information-sharing (last visited May 19, 2026).

proliferation of their sensitive and proprietary information.[395] Moreover, states have the option of using centralized emergency services planning or regulatory bodies to issue the requests and then coordinating with local agencies and sharing information when necessary, consistent with § 4.2. This approach also aligns with our determination to permit filing 911 reliability certifications at the level of a given state or territory, rather than on the previous PSAP-by-PSAP level.

We further clarify that certain of the NORS procedures for accessing information may not apply in every circumstance in the 911 reliability context. For example, rules governing agencies' account access to the NORS database will not apply unless and until the Bureau establishes a pathway for direct 911 Authority access to any new reliability database. Instructions pertaining to agency submissions to the Bureau also will not apply, because our framework implements a process carried out through the cooperation of CSPs and 911 Authorities. We believe that CSPs and 911 Authorities, working together in good faith, will be able to adapt the NORS procedures to their specific circumstances straightforwardly, altering them by mutual agreement as necessary. And consistent with the NORS framework, the Bureau may use its delegated authority to terminate a 911 Authority's right of access to CSP certifications for a period of time, among other measures, if the 911 Authority violates its confidentiality obligations.[396]

Access procedures. State, territorial, and tribal 911 Authorities may obtain copies of filings submitted by the CSPs that provide them with covered services or that operate covered 911 circuits or paths located within their jurisdictions. A 911 Authority may request copies from CSPs directly, in which case the CSP must comply within 14 days, provided the 911 Authority signs a confidentiality agreement that is consistent with the confidentiality protections for reports

---

[395] *Accord NORS Information Sharing Order*, 36 FCC Rcd at 6144-45, para. 27; *see also* Lumen Comments at 13, n.42 (recommending that the Commission "reinforce that access to these certifications would be limited to '911 Authorities' and not 'state and local governments' writ large").
[396] *See* 47 CFR § 4.2(e); 47 CFR § 0.392(j).

filed in NORS.[397] CSPs may omit or redact information relating to portions of their networks or facilities that do not provide covered services to, and are not located in, the requesting 911 Authority's jurisdiction. CSPs' obligation to produce certifications and reports to 911 Authorities will commence following the announced deadline for submitting such certifications and reports.

We also authorize state, territorial, and tribal 911 Authorities to obtain certifications and reports filed in 911RCS from the Bureau.[398] We direct the Bureau to provide instructions, updated as necessary, to 911 Authorities regarding access to such filings.[399] To conserve Commission resources, we allow 911 Authorities to obtain certifications from the Bureau only after attempting to obtain them directly from CSPs, and we will not require Bureau staff to redact CSP filings. For the same reason, we reject requests from several commenters that the Commission should make itself the *only* source from which 911 Authorities can obtain CSP certifications.[400]

Remediation Process

In the *NG911 Reliability FNPRM*, the Commission proposed to codify the remediation process by which the Bureau addresses apparent deficiencies in CSP reliability certifications.[401] Although the Bureau already has delegated authority to conduct remediation, the Commission suggested that adopting codified procedures would make the remediation process more transparent and predictable.[402]

We find that codification of our remediation procedures will increase awareness of how the Bureau determines violations of § 9.19(b) and of providers' ability to contest such findings. No

---

[397] *See* 47 CFR § 4.2.
[398] *See* 47 CFR § 0.392(i) and (j).
[399] *See* NASNA Comments at 7 (urging the Commission to "make[] the access permission/approval process both simple and secure for state and local units of government. While transparency that provides security is appreciated, systems that are burdensome create barriers to that transparency.").
[400] *See* Lumen Comments at 14; Home Telephone Comments at 14.
[401] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2709-10, paras. 105-110.
[402] *Id*.

commenters oppose codification, and COPUC strongly supports the proposed procedures.[403] COPUC also proposes that the codified procedures provide for 911 Authorities to receive copies of all Bureau remediation notices provided to CSPs in their jurisdictions [404] We agree with COPUC's proposal and include it in the codified procedures.

When the Bureau identifies apparent noncompliance with the requirement for CSPs to provide reliable 911 service, it ordinarily will try to work with the provider and other interested stakeholders (e.g., affected PSAPs) to address any shortcomings.[405] The Bureau also may order the provider to take remedial action.[406] We codify the following remediation procedures that the Bureau and CSPs will follow in such cases:[407]

- *Notice*. If a CSP's certification or other information indicates that it may not have taken reasonable measures as required by § 9.19(b), the Bureau may issue and electronically serve on the CSP a notice describing its apparent deficiencies and any remedial actions the Bureau proposes. The notice may include requests for relevant documents and information.
- *Response*. The CSP must provide any requested documents and information to the Bureau within 30 days. It may also submit a written response to the notice.
- *Order*. At any point after the 30th day following its service of the notice, the Bureau may issue and serve on the CSP an order setting forth its findings and specifying the remedial actions the CSP must take. The order also may set deadlines for the required actions and identify information the CSP must submit to demonstrate its compliance with the order.
- *Notice to 911 Authorities*. The CSP must deliver a copy of the Bureau's order promptly to the 911 Authority for each jurisdiction in which its reliability measures were found

[403] COPUC Comments at 12 ("It does little good to have a CSP report its noncompliance to the Commission if no action is taken to resolve the issue.").
[404] *Id*.
[405] *911 Reliability Order*, 28 FCC Rcd at 17497, para. 63.
[406] *Id.*; 47 CFR § 0.392(j).
[407] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2709, paras. 105-07.

deficient or in which it was directed to take remedial actions.[408]

This process accurately reflects current practice, and it falls within the broad scope of the authority the Commission already has delegated to the Bureau.[409] We also clarify that the newly-codified process described above applies solely to the remediation of violations of §9.19(b) by the Bureau and does not limit the Bureau's general administrative authority over the 911 reliability framework or constrain the Bureau's ability to take other enforcement or oversight actions pursuant to its delegated authority. Nor does the remediation process constrain the Commission's broader adjudication or enforcement authorities, including its statutory powers to enforce its orders and to assess forfeitures, whether on referral from the Bureau or otherwise.[410]

Other issues

Consumer portal and petition process. In the *NG911 Reliability FNPRM*, the Commission sought comment on establishing a new consumer portal dedicated to 911-related outage reports and a new petition process for 911 Authorities to allege CSP violations of the 911 reliability framework and interoperability measures.[411] The Commission suggested these mechanisms as potential complements to the existing avenues through which consumers and 911 Authorities already may report 911 reliability issues to the Bureau's attention.[412] On review of the record, however, we decline to adopt these proposals.

Comments are mixed in favor of and against establishing a new petitions process or a

---

[408] *See* Appendix A (§ 9.20(g)); COPUC Comments at 12 ("The 911 Authority is in the best position to monitor the activity of the CSP to ensure that it is complying with the Bureau's order, but only if it knows that such an order exists.").

[409] 47 CFR § 0.392(j).

[410] *See*, *e.g.*, 47 U.S.C. § 401(b) (authority to enforce orders); 47 U.S.C. §§ 503-504 (forfeitures); 47 CFR § 1.2 (issuance of declaratory rulings); *911 Reliability Order*, 28 FCC Rcd at 17495, para. 55 ("[T]he reliability certifications [are] subject to penalties for false or misleading statements[.]") (citing 18 U.S.C. § 1001 (false statements to the federal government) and 47 CFR § 1.17 (truthful and accurate statements to the Commission)). The Public Safety and Homeland Security Bureau may refer noncompliant CSPs to the Enforcement Bureau, for example, but typically will not do so if a provider is acting in good faith. *911 Reliability Order*, 28 FCC Rcd at 17497, para. 63.

[411] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2703 and 2709-10, paras. 89 and 108-09.

[412] *See*, *e.g.*, *NG911 Reliability FNPRM*, 40 FCC Rcd at 2703 and 2709, paras. 89 and 108 (proposing to remind 911 Authorities that they "may continue to informally refer alleged 911 reliability and interoperability deficiencies to the Bureau without a formal petition"). *See also* FCC, Consumer Inquiries and Complaints Center, https://consumercomplaints.fcc.gov/hc/en-us (last visited May 19, 2026); FCC, Public Safety Support Center, https://www.fcc.gov/general/public-safety-support-center (last visited May 19, 2026).

dedicated consumer portal. Supporters argue that a new petition process would encourage frank exchanges between 911 Authorities and CSPs and that a new consumer portal would increase transparency and enhance communication between the Commission and the public.[413] However, a number of commenters, including Verizon, Intrado, and CTIA, believe that a petition process would be more likely to spoil coordination and cooperation among stakeholders and undermine the ability of Bureau staff to have candid and constructive discussions with providers.[414] They also contend that the new complaint mechanisms would be duplicative of existing avenues through which concerns about 911 service and CSP compliance can be raised, including the Public Safety Support Center (for PSAPs and 911 Authorities), the Consumer Inquiries and Complaints Center (for individual consumers), and the Commission's general petition process.[415] CTIA argues that the new mechanisms therefore would impose substantial costs without significant countervailing public benefits.[416]

We are persuaded that consumers and 911 Authorities can provide significant value by identifying localized reliability concerns and assisting the Commission's oversight of NG911 networks, but we conclude that these benefits can be fully achieved through the Commission's existing reporting avenues and informal referral processes. Rather than create new procedural mechanisms, which the record shows could impose unnecessary burdens, we will continue to rely on these established channels to facilitate communication, surface potential violations, and support cooperative engagement between the Bureau, CSPs, 911 Authorities, and the public. To ensure that our existing channels are used to their greatest benefit, we instruct the Bureau to consider undertaking targeted outreach and engagement efforts to raise awareness of these avenues and to encourage 911 Authorities and consumers to use them to refer concerns relating

[413] Lumen Comments at 15-16; Public Knowledge Comments at 8; COPUC Comments at 12; CCOA Reply at 4.
[414] *See*, *e.g.*, Verizon Comments at 17.
[415] CTIA Reply at 7, 10; Verizon Comments at 16; Intrado Reply at 8-9. CTIA and Verizon also express concern that encouraging petitions from individual state 911 Authorities could lead to reliability standards being enforced unevenly across jurisdictions. CTIA Reply at 7; Verizon Comments at 16 ("[T]he FNPRM's proposed enforcement regime leaves the door open to localized second-guessing of otherwise reasonable measures.").
[416] CTIA Comments at 8.

to the reliability of covered 911 services.

Cessation notices. We do not adopt the Commission's proposal to require CSPs to notify 911 Authorities, at the same time they notify the Commission, when they cease providing covered 911 services.[417] Under the previous 911 reliability rules, CSPs must file a notification with the Commission under penalty of perjury no later than 60 days after their cessation of service.[418] The cessation notifications to the Commission become due "only when a [CSP] completely ceases providing covered 911 services" and not whenever it ceases to provide service to a particular PSAP or jurisdiction.[419] Accordingly, only the last jurisdiction where a CSP retires its last covered 911 service or facility would receive the notice. We therefore find that the limited potential benefit to 911 Authorities from receiving the notifications would not outweigh the additional burden on all CSPs to maintain awareness of a new notification requirement. We note as well that no commenters responded to this proposal in the record.

PSAP Outage Notifications. Finally, we note that § 4.9(h) of the rules incorporates section 9.19's definition of "covered 911 service provider" in defining the providers that must notify 911 special facilities about certain outages. We decline at this time to extend the section 4.9(h) reporting obligation to those entities that are newly designated as CSPs by this *Order*.[420] Several commenters contend that requiring newly-designated CSPs to provide outage notifications to PSAPs is unnecessary or possibly counterproductive, as it could lead to duplicative notifications to PSAPs.[421] It is also unclear from the record whether it is technically feasible for operators of multi-OSP LISs and LNGs, major IP transport facilities, and IP 911 traffic aggregation facilities to notify 911 special facilities about outages that potentially affect them as our rules require. Because the current record is mixed and does not contain a thorough discussion of these issues,

---

[417] *Cf. NG911 Reliability FNPRM*, 40 FCC Rcd at 2708-09, para. 104.
[418] 47 CFR § 9.19(d)(4).
[419] *Id*.
[420] *See* 47 CFR § 4.9(h).
[421] *See*, *e.g.*, Comtech Comments at 20 (arguing against "a one-size-fits-all notification requirement applicable to every CSP involved in an NG911 call flow"); iCERT Reply at 7; BRETSA Reply at 2; Intrado Comments at 8-9 (additional notifiers "would multiply the number of notifications PSAPs receive"); DATAMARK Reply at 5; T-Mobile Comments at 2-3.

we agree with commenters that further consideration is warranted and therefore do not require these operators to report at this juncture.[422] We note that cable, satellite, wireless, legacy wireline, interconnected VoIP, as well as covered 911 service providers (as previously defined), continue to have a non-delegable duty to provide notification to 911 special facilities under our rules, and that reliance upon a third party to contribute to 911 call processing does not relieve the provider of that duty.[423]

Compliance Timelines

We establish an 18-month transition period for phasing in our new 911 reliability framework and interoperability measures. We find that this transition period is justified to avoid excessive costs, allow operational flexibility, and provide time for stakeholders to gain experience with implementing reliability measures and interoperability arrangements in NG911 networks as deployments continue to mature.[424] The 18-month period will commence when the Bureau issues a public notice announcing approval by the Office of Management and Budget (OMB) of the information collection requirements adopted in this Order. Newly designated CSPs will have six months from the public notice date to file an attestation with the Commission identifying themselves as CSPs.[425] All IP-based CSPs will have 18 months from the public notice date to come into compliance with the updated reliability benchmarks for physical diversity, operational integrity, and network monitoring, or to implement alternative measures. CSPs covered by the 2013 rules will continue to be subject to the reliability benchmarks established under those rules. CSPs that have previously filed annual certifications under the

---

[422] *See*, *e.g.*, APCO Reply at 15 ("[O]utage reporting requirements warrant a more in-depth review beyond the scope of the current . . . proceeding."); NENA Comments at 26; CTIA Reply, at 6-7; Comtech Comments at 20 (requesting a "dedicated proceeding" that considers "prior Commission findings, . . . CSRIC VI best practices, as well as current NENA guidance"); iCERT Reply 7; Verizon Reply at 3; Motorola Reply at 5.

[423] *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, Improving 911 Reliability, New Part 4 of Commission's Rules Concerning Disruptions to Communications*, PS Docket Nos. 15-80 and 13-75, ET Docket No. 04-35, Second Report and Order, 37 FCC Rcd 13847, 13854-55, para. 13 (2022). *See id*. at 13859, para. 20 ("We expect service providers to address these responsibilities within their 911 service contracts with third parties as needed.").

[424] *See* City of Coconut Creek, FL July 21, 2025 Comments at 1 ("We respectfully recommend that the FCC provide flexible and realistic timelines for compliance[.]").

[425] "Newly designated CSPs" are those providers classified as CSPs under the updated rules that did not file certifications as CSPs under the 2013 reliability rules.

2013 rules will not be required to file additional annual certifications during the transition period. All CSPs will file their initial reliability certifications and interoperability reports pursuant to the updated rules 18 months from the public notice date.[426]

Legal Authority

We find our approach this *Order* to strengthen the reliability and interoperability of NG911 falls squarely within the legal authority that Congress has delegated to the Commission. Congress has enacted numerous provisions in the Communications Act of 1934, as amended (the Act), and other 911-related statutes "that, taken together, establish an overarching federal interest in ensuring the effectiveness of the 911 system."[427] The Commission has been granted broad authority, for example, to "promot[e] safety of life and property through the use of wire and radio communications,"[428] including through use of the nation's 911 system.[429] The Commission's public safety interest is among its most important responsibilities, and it informs the Commission's exercise of its other statutory authority pursuant to Congress's other directives. The D.C. Circuit consistently has affirmed the Commission's duty to consider public safety under the Communications Act and to impose obligations to protect public safety in the

---

[426] Entities that begin providing covered 911 services after the initial certification and reporting deadline must submit an initial reliability certification and interoperability report when they begin providing services.

[427] *See, e.g.*, *911 Fee Diversion*; *New and Emerging Technologies 911 Improvement Act of 2008*, PS Docket Nos. 20-291 and 09-14, Report and Order, 36 FCC Rcd 10804, 10810-11, para. 16 & n.41 (2021) (*911 Fee Diversion Order*); *NG911 Transition Order*, 39 FCC Rcd at 8206-07, para. 154.

[428] 47 U.S.C. § 151. The Communications Act authorizes the Commission to make rules and regulations, issue orders, and prescribe restrictions and conditions that are consistent with the provisions of the act. *See, e.g.*, 47 U.S.C. §§ 154(i) and 303(r).

[429] *See*, *e.g.*, *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102, Report and Order and Second Further Notice of Proposed Rulemaking, 18 FCC Rcd 25340, 25345, para. 13 (2003) ("We find that Congress has given the Commission broad authority to deal with public safety concerns in wire and radio communications."); *Revision of the Commission's rules to ensure compatibility with enhanced 911 emergency calling systems*, CC Docket No. 94-102, Notice of Proposed Rule Making, 9 FCC Rcd 6170, 6171, para. 7 (1994) ("It is difficult to identify a nationwide wire or radio communication service more immediately associated with promoting safety of life and property than 911."); *Nuvio Corp. v. FCC*, 473 F.3d 302, 312 (D.C. Cir. 2006) (Kavanaugh, J., concurring) (stating that Congress has granted the Commission "broad public safety and 911 authority"). Moreover, in the Net 911 Act's legislative history, Congress recognized that "[s]hould changes in the marketplace or in technology merit, the Committee expects that the Commission will reexamine its regulations as necessary, consistent with the Commission's general authority under section 1 of the Communications Act of 1934 to promote the 'safety of life and property' through the use of wire and radio communications." H.R. Rep. No.110-442, at 13 (Nov. 13, 2007), https://www.govinfo.gov/app/details/CRPT-110hrpt442.

public interest.[430] Beyond this general mandate, section 251(e)(3) of the Communications Act makes the Commission responsible for establishing 911 as the universal emergency telephone number for both wireline and wireless telephone service,[431] demonstrating Congress's intent to grant the Commission broad authority for "ensuring that 911 service is available throughout the country."[432] In a subsequent statute, Congress found that "for the sake of our Nation's homeland security and public safety, a universal emergency telephone number (911) that is enhanced with the most modern and state-of-the-art telecommunications capabilities possible should be available to all citizens in all regions of the Nation."[433]

Moreover, to the extent that covered 911 service providers are common carriers, section 201(b) of the Communications Act requires them to adopt "practices" that are "just and reasonable" and authorizes the Commission to "prescribe such rules and regulations as may be necessary in the public interest" to enforce that requirement.[434] The Commission also may require carriers "to provide [themselves] with adequate facilities for the expeditious and efficient performance of [their] service[s]" when "reasonably required in the interest of public convenience and necessity."[435] The Commission consistently has relied on these authorities to regulate the provision of 911 service, including when it adopted the 2013 reliability rules.[436] Similar provisions empower the Commission to regulate the adequacy of the services provided by wireless and interconnected VoIP providers.[437] Based on the record, we find that the 911

---

[430] *See, e.g.*, *Nuvio Corp.*, 473 F.3d at 307-08 (upholding new E911 requirements on the basis of, in part, the Commission's statutory duty to "'promot[e] safety of life and property through the use of wire and radio communications'" (quoting 47 U.S.C. § 151; emphasis omitted)); *U.S. Cellular Corp. v. FCC*, 254 F.3d 78, 85 (D.C. Cir. 2001) (upholding the Commission's E911 default cost allocation rule based in part on the fact that "the Commission . . . imposed upon wireless carriers an obligation to implement a service in the public interest").
[431] 47 U.S.C. § 251(e)(3).
[432] *Nuvio Corp.*, 473 F.3d at 311 (Kavanaugh, J., concurring).
[433] ENHANCE 911 Act of 2004 § 102, 47 U.S.C. § 942, note.
[434] 47 U.S.C. § 201(b).
[435] 47 U.S.C. § 214(d).
[436] *See*, *e.g.*, *911 Reliability Order*, 28 FCC Rcd at 17529, para. 149.
[437] 47 U.S.C. § 303 ("[T]he Commission . . ., as public convenience, interest, or necessity requires, shall . . . (b) [p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class" [and] "(r) [m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter") (wireless carriers); 47 U.S.C. § 615a-1 ("(a) It shall be the duty of each IP-enabled voice service provider to provide 9-1-1 service and enhanced 9-1-1 service to its subscribers in accordance with the requirements of the [FCC];" "(c) The Commission . . . (3) may modify such regulations from time to time, as necessitated by changes in the market or technology, to ensure the

reliability and interoperability practices and facilities addressed in this *Order* are just and reasonable, serve the public interest, and are required for public convenience and necessity.

We also conclude that this *Order* falls within the Commission's broad authority under the Twenty-First Century Communications and Video Accessibility Act (CVAA) to regulate the provision of NG911 services specifically.[438] Congress enacted the CVAA to ensure that people with disabilities have "equal access to emergency services . . . as a part of the migration to a national [IP]-enabled emergency network[.]"[439] To further that goal, Congress required the FCC to establish an Emergency Access Advisory Committee (EAAC) to recommend "the most effective and efficient technologies and methods" by which to achieve the CVAA's purpose, and Congress provided the Commission "the authority to promulgate regulations to implement the recommendations proposed by the [EAAC]."[440] Congress also authorized the Commission to promulgate "any other regulations, technical standards, protocols, and procedures as are necessary to achieve reliable, interoperable communication that ensures access by individuals with disabilities to an [IP]-enabled emergency network, where achievable and technically feasible."[441] Ensuring the reliability and interoperability of the nation's NG911 network therefore is one of the Commission's key mandates under the CVAA.

Our approach comports with the CVAA's mandate because it enhances the reliability and interoperability of the nation's NG911 network—the IP-enabled emergency network addressed in the CVAA—and is achievable and technically feasible. We (1) identify which services and facilities are the most critical to modern NG911 networks; (2) establish reasonable reliability standards for the providers of these services and facilities based on prevailing best practices; (3) require CSPs to take reasonable measures to enable interoperability between ESInets and NGCS facilities; and (4) improve oversight processes. These changes are designed to reduce NG911

---

ability of an IP-enabled voice service provider to comply with its obligations under subsection (a)[.]") (VoIP providers).

[438] Twenty-First Century Communications and Video Accessibility Act of 2010, 47 U.S.C. § 609 et seq.

[439] 47 U.S.C. § 615c(a).

[440] 47 U.S.C. § 615c(c), (g).

[441] 47 U.S.C. § 615c(g).

service outages, thereby increasing access to IP-based 911 services for people with disabilities, including multimedia capabilities that cannot be supported on legacy TDM-based networks.[442] Indeed, one of EAAC's recommendations to the Commission was to ensure an "[a]ccessible NG9-1-1 Network" that could "support features, functions and capabilities . . . to enable individuals with disabilities to make multimedia NG9-1-1 emergency calls."[443] These advanced 911 features currently are the least likely to be supported by existing interoperability measures, and users of these services therefore stand to benefit most from the 911 reliability framework and interoperability measures we adopt today.[444] The EAAC also recommended that the FCC promote interoperability by allowing NG911 providers "to identify the formats for their environment[s]" and to "convert these formats where their environments interface with other environments[.]"[445] That is the approach we have taken—requiring providers to use reasonable efforts to enable interoperability, while affording them flexibility to determine the formats in which they will do so.

As the Commission has recognized consistently in prior rulemakings, the Commission's regulatory authority under the CVAA is not limited to services that are used exclusively by people with disabilities.[446] Nor does the CVAA "requir[e] the FCC to ensure that any rules we adopt confer zero benefits on consumers outside the disability community[.]"[447] Rather, we adhere to and advance the CVAA's mandate precisely because they promote NG911 reliability

---

[442] *See* Emergency Access Advisory Committee, Report and Recommendations, at 21-25 (Dec. 7, 2011), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-312161A1.doc (*EAAC Report*) (describing NG911 functions that can benefit persons with disabilities).
[443] *EAAC Report* at 19 (Recommendation P1.1).
[444] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2696-97, 2700, paras. 71, 83 (NASNA's 2020 Interoperability Matrix showed higher levels of interstate interoperability for 911 voice calls but no or low levels of interstate interoperability for multimedia emergency services features that enhance accessibility).
[445] *EAAC Report* at 20 (Recommendation P1.4).
[446] *NG911 Transition Order*, 39 FCC Rcd at 8208, para. 157; *see also*, *e.g.*, *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, PS Docket Nos. 11-153, 10-255, Report and Order, 28 FCC Rcd 7556, 7598, para. 119 (2013) (*Bounce-Back Order*) ("[T]he FCC has authority under the CVAA to require action that is not limited to the disability community."); *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications*; *Framework for Next Generation 911 Deployment*, PS Docket Nos. 11-153, 10-255, Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd 9846, 9878, para. 71 (2014) (*T911 Second Report and Order*) (affirming that "the CVAA vests the Commission with direct authority to impose 911 bounce-back requirements on both CMRS providers and other providers of interconnected text messaging applications, including [over-the-top] providers").
[447] *T911 Second Report and Order*, 29 FCC Rcd at 9878, para. 71.

equally between people with and without disabilities on a platform-neutral basis. Moreover, the EAAC concluded that people with disabilities may depend on the same voice services as those without disabilities in emergency situations,[448] or they may rely on a caretaker or other persons using such services.[449] We believe we should broadly cover different types of service providers to ensure that persons with disabilities have full and equal access to emergency services when they are needed.

We also find that our approach to improve the reliability certification process is authorized under section 218 of the Act, which allows the Commission to "inquire into the management of the business of all carriers" and to obtain from them "full and complete information necessary to enable the Commission to perform the duties and carry out the objects for which it was created."[450] Furthermore, section 4(n) of the Act states that "[f]or the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property," the Commission "shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems."[451] The Commission previously has relied on section 4(n) in similar contexts, for example, as providing authority to require interconnected VoIP providers to report outages and to require emergency alerting plans to allow the Commission and other stakeholders to review and identify gaps in emergency alerting architecture and to take measures to address these shortcomings.[452] The Commission also has authority under the NET 911 Act to "compile . . .

---

[448] *EAAC Report* at 19 (Recommendation P1.2); *see id.* at 14 (finding that 14.7% of persons with disabilities have a "mobility disability that does not affect [their] ability to use communications devices"). The EAAC found that respondents to its survey "overwhelmingly want to be able to call PSAPs using the same technologies they use daily and know how to use reliably (just as all other citizens can)." *Id.* at 19 ("Users need to use familiar technologies and methods, such as text/ audio/ video communication, when calling in an emergency and therefore both want and need to be able to access NG9-1-1 from the same devices they will use every day.").

[449] *See also Bounce-Back Order*, 28 FCC Rcd at 7598, para. 120 ("In emergency situations, persons with disabilities may need to access emergency services quickly and this may require them to use mobile devices owned by others.").

[450] 47 U.S.C. § 218. *See also* 47 U.S.C. § 303(j) (authorizing the Commission to issue rules and regulations requiring wireless licensees to keep records of "programs, transmissions of energy, communications, or signals").

[451] 47 U.S.C. § 154(n).

[452] *Ensuring the Reliability and Resiliency of the 988 Suicide & Crisis Lifeline; Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications; Implementation of the National Suicide Hotline Improvement Act of 2018*, PS Docket Nos. 23-5, 15-80, Report and Order, 38 FCC Rcd 6917, 6945, para. 50 & n.190 (2023) (citing *The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to*

information concerning 9-1-1 and enhanced 9-1-1 elements, for the purpose of assisting IP-enabled voice service providers in complying with this section."[453] Thus, we conclude that, as part of a cooperative governance structure for 911, "the Commission is authorized to gather and disseminate information from carriers and other regulatees for the purpose of ensuring effective public safety communications," including by allowing 911 Authorities to access CSP reliability certifications to assist with oversight.[454]

Together, the foregoing statutes confirm the Commission's authority and responsibility to establish and maintain a comprehensive and effective 911 system.[455] They give the Commission broad authority to ensure that the 911 system is available and accessible and functions effectively to process and deliver 911 calls and texts from all people in need of aid using any type of service; authorize the Commission to adopt the framework and measures herein; and represent the repeated endorsement by Congress of the Commission's ability to act in this context.[456] The Commission previously concluded that "[i]n light of these express statutory responsibilities, regulation of additional capabilities related to reliable 911 service, both today and in an NG911 environment, would be well within Commission's . . . statutory authority."[457] The Commission also has stated that it "already has sufficient authority to regulate the 911 and NG911 activity of, *inter alia*, wireline and wireless carriers, interconnected VoIP providers, and other IP-based service providers" and that its jurisdiction to regulate 911 extends to the regulation of NG911 across different technologies.[458] The Commission sought comment on this legal framework in the *NG911 Reliability FNPRM*,[459] and no commenter argues that the proposed NG911 reliability

---

Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers, PS Docket No. 11-82, Report and Order, 27 FCC Rcd 2650, 2676, para. 61 (2012)).

[453] 47 U.S.C. § 615a-1(g).

[454] *2014 Reliability NPRM*, 29 FCC Rcd at 14235, para. 78.

[455] *911 Fee Diversion Order*, 36 FCC Rcd at 10810-11, para. 16.

[456] *Id.*

[457] *911 Reliability Order*, 28 FCC Rcd at 17529, para. 150.

[458] FCC, *Legal and Regulatory Framework for Next Generation 911 Services, Report to Congress and Recommendations*, section 4.1.2.2 (Feb. 22, 2013), https://docs.fcc.gov/public/attachments/DOC-319165A1.pdf; *2014 Reliability NPRM*, 29 FCC Rcd at 14223, para. 34 ("[T]he Commission has the public safety imperative to oversee each of the increasingly complex component pieces of the nation's 911 infrastructure.").

[459] *See*, *e.g.*, *NG911 Reliability FNPRM*, 40 FCC Rcd at 2714, para. 117.

framework exceeds the Commission's statutory authority.

The Commission historically has shared authority over the 911 system with state, local, and tribal governments, which exercise their oversight through various types of agencies, such as public safety agencies and, in some cases, state public utility commissions (PUCs).[460] These agencies play critical roles in ensuring that 911 is available when needed, including by "establishing and designating PSAPs or appropriate default answering points, purchasing customer premises equipment, retaining and training PSAP personnel, purchasing 911 network services, and implementing a cost recovery mechanism to fund all of the foregoing."[461] Congress recognized the important role that states and localities can play in ensuring reliable 911 service when it directed the Commission to "encourage and support efforts by States" in this area.[462] We reaffirm the Commission's policy to support efforts by states and localities to deploy comprehensive end-to-end emergency communications infrastructure and programs, including seamless, ubiquitous, and reliable 911 service.[463]

We find that our approach strikes an appropriate balance between federal guidance and state and local autonomy. As discussed above, we do not alter state jurisdiction over 911 or directly affect intrastate facilities. We continue to specifically exempt PSAPs and other governmental entities from 911 reliability obligations, and they empower 911 Authorities by ensuring them access to the reliability certifications of CSPs in their states. We also focus on interstate facilities within multistate 911 networks that no individual state can regulate effectively. Specifically, the new CSP classes we identify operate facilities that often extend across state boundaries.[464] Similarly, the ESInet interoperability requirement we adopt applies to

---

[460] *NG911 Transition Order*, 39 FCC Rcd at 8212, para. 164.
[461] *2014 911 Reliability NPRM*, 29 FCC Rcd at 14218, para. 28 (quoting *IP-Enabled Services*; *E911 Requirements for IP-Enabled Service Providers*, WC Docket Nos. 05-196, 04-36, First Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 10245, 10249, para. 7 (2005)).
[462] 47 U.S.C. § 615 (directing the Commission to "encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated statewide plans, including seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 911 service").
[463] *2014 911 Reliability NPRM*, 29 FCC Rcd at 14210, para. 4; *id.* at 14220, para. 34.
[464] For example, 911 traffic aggregation facilities, multi-OSP LISs and multi-OSP LNGs collect 911 traffic from multiple OSPs that may be located in different states and process and transport the traffic for ultimate delivery to ESInets POIs in various states across the country.

interstate communications. Consistent with past practice, we intend to partner with state, local, and tribal 911 Authorities while respecting their unique interest in the delivery of 911 service to their communities.

Commenters generally agree with our analysis and characterize our approach as an appropriate exercise of federal authority over 911 systems that also respects the power of state, local, and tribal 911 Authorities to oversee the 911 network infrastructure within their jurisdictions. Colorado's PUC, for example, believes our approach is consistent with the Commission's historic approach of "set[ting] a baseline for 911 networks and call delivery and the states add[ing] to this through statute, regulation, and service level agreements in order to address their own particular needs."[465] NASNA similarly states that the Commission's role includes protecting the integrity of NG911 systems by requiring CSPs to supply all critical elements of NG911 systems to best practice standards, while 911 Authorities' role is "to define their procurement requirements and their system elements."[466] APCO agrees, noting that the new reliability rules are not intended to alter states' jurisdiction over 911 or directly affect their intrastate facilities.[467]

Another commenter, while "recogniz[ing] the need for clear rules that promote the reliability of interconnections . . . for reliable routing of emergency 911 calls," seeks clarification about the scope of state and local oversight of 911 reliability.[468] We clarify that the Commission

---

[465] COPUC Comments at 2 ("[T]he Commission and the states have successfully shared concurrent jurisdiction regarding 911 call delivery, and COPUC hopes that this amicable arrangement will continue.").
[466] NASNA Comments at 6 ("We believe that CSPs should not be permitted under the rules to omit critical functional elements during procurement and then lay the responsibility at the feet of the local 911 jurisdiction citing *caveat emptor*.").
[467] APCO Reply at 11-12. NTCA and the RLEC Parties claim that the Commission previously characterized NG911 calls as purely "intrastate" in nature. *See* NTCA and the RLEC Parties Comments at 3 (citing *NG911 Transition Order*, 39 FCC Rcd at 8212-13, para. 165). In reality, the Commission was describing its federal/state cost allocation rules, which "treat the costs of transmitting these [911] calls as jurisdictionally intrastate" when the caller and call recipient are located in the same jurisdiction. *NG911 Transition Order*, 39 FCC Rcd at 8212-13, para. 165 & n. 492 (citing 47 CFR parts 32, 36, 61, 65, and 69). The Commission has long recognized "that the technologies and commercial relationships that form the foundation of the 911 system are transitioning [to NG911] and, as a result, becoming increasingly interstate in nature." *2014 911 Reliability NPRM*, 29 FCC Rcd at 14208, para. 2. *See also* APCO Reply at 11-12 ("In an NG9-1-1 environment, calls and associated data can, and often must, cross state boundaries. The artificial division between 'interstate' and 'intrastate' interoperability has no practical basis in the NG9-1-1 ecosystem . . . given the inherently interconnected and borderless nature of NG9-1-1 traffic.").
[468] NTCA and the RLEC Parties Comments at 3-4.

has sole authority to enforce the 911 reliability requirements for CSPs codified in part 9 of the Commission's rules. Through the Bureau, the Commission determines whether CSP certifications are timely and accurate and whether CSPs' network implementations comply with the reliability benchmarks or otherwise are reasonable alternative measures. We recognize, however, that 911 Authorities have a shared interest in ensuring the delivery of reliable 911 service to their constituents. Accordingly, we encourage 911 Authorities to make the Commission aware of any potential violations of the Commission's 911 reliability framework in their jurisdictions, and as discussed above, we allow them access to CSPs' reliability certifications to aid in that effort.

We further clarify that 911 Authorities may independently require NG911 operators in their jurisdictions to provide services or to meet performance standards that differ from those described in this *Order*.[469] In such cases, the Commission will deem a CSP to be compliant with the part 9 rules if it truthfully certifies to implementing alternative measures that were mandated or approved by its 911 Authority. It then would fall to the 911 Authority to oversee the CSP's performance and to enforce its local requirements via its contractual rights or through its laws or regulations. To illustrate, Colorado regulates providers of "basic emergency service" to governing bodies and PSAPs within the state, which is defined to include the aggregation and transportation of 911 calls.[470] These providers are overseen in part by the Colorado Public Utilities Commission, and they must comply with reliability standards that overlap with—but are not identical to—the Commission's reliability framework in §9.19.[471] The Commission will accept, for example, a reliability certification from a Colorado CSP explaining that it has implemented alternative measures in lieu of a Commission benchmark because the measures were approved by the Colorado Public Utilities Commission as part of the provider's required

---

[469] For example, 911 Authorities commonly require five nines reliability in their service level agreements with NGCS providers.
[470] *See* 4 Colo. Code Regs. § 723-2-2131; Colo. Rev. Stat. § 40-15-201(2); 4 Colo. Code Regs. § 723-2:2130(b).
[471] *See*, *e.g.*, 4 Colo. Code Regs. § 723-2:2143 (requiring basic emergency services providers to "take reasonable measures to provide reliable BES including circuit diversity, central-office backup power, and diverse network monitoring" as well as other measures).

biennial improvement plan.[472] Because our framework accommodates state decision-making, there should be no conflict between how the Commission and state and local authorities regulate 911 reliability or carry out their respective oversight roles and therefore no cause for preemption.[473]

Benefit and Cost Analysis

Benefits. The benefits of today's item exceed the costs. This *Order* will lead to improvements in coordination between 911 Authorities and CSPs, promote IP reliability best practices and system interoperability, enhance state and local government oversight, prevent delays in the NG911 transition, and reduce 911 call failures and outages. The elimination of annual certification requirements removes the costs of unnecessary and excessive filings which would serve little value towards realizing these benefits. The Commission has previously found that improving 911 reliability produces significant benefits for the protection of public safety and is consistent with the Commission's statutory charge to promote the safety of life and property through the use of wire and radio communications.[474] We also find that improving 911 reliability will advance national security objectives, as 911 outages leave first responders, including police, fire, and EMS agencies blind to unfolding threats, such as a terrorist attack.[475] Although sparse in quantitative estimates, the record in this proceeding supports our conclusion that the benefits of updated NG911 reliability framework and interoperability measures include empowering state and local governments to manage their NG911 deployments,[476] providing 911

---

[472] *See* 4 Colo. Code Regs. § 723-2:2143(b).

[473] In the *NG911 Transition Order*, the Commission similarly affirmed the right of 911 Authorities to adopt provisions concerning the implementation of NG911 that differ from the Commission's framework. *See NG911 Transition Order*, 39 FCC Rcd at 8140, para 7 ("[W]e recognize and do not preempt the long-standing authority of state and local government over the provision of 911 service. Thus, 911 Authorities at the state, local, and Tribal level remain free to establish alternative provisions within their jurisdictions for the implementation of NG911, definition of demarcation points, and allocation and recovery of costs."); *id.* at 8212-13, para. 165 ("There can be no preemption where there is no conflict or inconsistency between federal and state requirements.").

[474] *911 Reliability Order*, 28 FCC Rcd at 17500, 17502, paras. 73, 77; *NG911 Transition Order*, 39 FCC Rcd at 8221-22, 8226, paras. 185-186, 195.

[475] *See* Stephanie Armour, *The Nation's 911 System Is on the Brink of Its Own Emergency* (Jul. 16, 2024), https://www.usatoday.com/story/news/nation/2024/07/16/911-emergency-system-brink-of-crisis/74411456007/ ("Outages have hit at least eight states this year. . . 'This is a national security imperative. . . In a crisis – a school shooting or a house fire or, God forbid, a terrorist attack – people call 911 first . . . The system can't go down.'").

[476] NYSPSC Comments at 2; NASNA Comments at 6.

Authorities with visibility and oversight into the entire NG911 ecosystem,[477] and mitigating or preventing large-scale 911 outages.[478] Countervailing claims about risk of NG911 transition delay have been resolved by our modifications to the proposed interoperability benchmark, and replacing the proposed annual interoperability certification with a simplified one-time report.[479] While it is difficult to quantify these benefits, we find that the benefits of improved NG911 reliability, including the prevention of 911 outages, would create sizable benefits to the public safety; indeed, even if these measures result in the saving of only a single life per year, doing so would result in benefits that far exceed the modest costs of our approach.[480] We therefore conclude that the benefits of our actions exceed their costs.

Costs. Today's item will impose approximately $3 million annually and $2.1 million in one-time costs on private businesses.[481] We note that the estimated one-time and annual costs will phase in over the next four years after adoption of the *Order* during the NG911 transition, as NG911 networks gradually replace legacy TDM 911 networks.[482] Most of today's rule changes will impose little or no costs. The ESInet and NGCS CSP categories are clarifications or minor modifications of the rules adopted in the 2013 *911 Reliability Order*.[483] The rule updates adding CSP definitions for major IP transport facilities operators, IP 911 traffic aggregation facilities operators, LIS operators, and transitional gateway operators represent minimal changes to keep pace with technology evolution and ensure realization of the benefits of the *NG911 Transition*

---

[477] NENA Comments at 1-2; Brian Rosen Reply at 2; CCOA Comments at 2.
[478] COPUC Comments at 2; NYSPSC Comments at 1-2; Palmetto Broadband Coalition Reply at 2-3.
[479] T-Mobile Reply at 7.
[480] While we do not attempt to place a value on human life, we note that the value of reducing the mortality risk is approximately $14.2 million per life saved, using a methodology developed by the U.S. Department of Transportation (DOT) that the Commission has relied on in past orders. *See* U.S. Department of Transportation, *Departmental Guidance on Valuation of a Statistical Life in Economic Analysis* (Mar 20, 2026), https://www.transportation.gov/office-policy/transportation-policy/revised-departmental-guidance-on-valuation-of-a-statistical-life-in-economic-analysis).
[481] The annual recurring cost of $3 million includes $1.8 million in transport diversity cost, $210,000 for operational integrity collocation cost, $260,000 for IP network monitoring cost, $260,000 for interoperability cost, and $481,560 in certification costs. The $2.1 million one-time cost includes: $600,000 in network routers for IP path diversity, $200,000 in servers and uninterruptible power supply (UPS) devices for operational integrity, $200,000 for IP network monitoring cost, $200,000 for interoperability cost, and $875,568 software, engineering, and installation labor one-time cost.
[482] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2717, para. 126.
[483] *911 Reliability Order*, 28 FCC Rcd at 17489-91, paras. 36-37 & n.85, para. 43; *see also NG911 Reliability FNPRM*, 40 FCC Rcd at 2717, 2719, paras. 124, 128.

Order.[484] Today's modifications to substantially reduce the number of entities included in the *NG911 Reliability FNPRM's* proposed covered 911 service classes of major IP transport, LIS operators, and transitional gateway operators further ensure costs will be minimal. In addition, the IP path diversity and IP monitoring benchmarks we adopt today are largely codifications of the rule interpretations adopted in the *2015 911 Reliability Recon. Order*.[485] Furthermore, both of those benchmarks and the operational integrity benchmark also codify CSRIC's recommendations of NG911 reliability tools that were already available or not overly burdensome to implement based on consideration of impacts on operations and capital budgets, labor costs, and service downtimes for upgrades.[486] The addition of a one-time interoperability report represents a minor update to account for rapidly moving technology.[487] Today's clarifications and modifications to the *NG911 Reliability FNPRM's* proposed IP diversity benchmark will further reduce estimated costs. We are also preserving flexibility for CSPs to implement alternate reliability practices based on engineering decisions in the field, and in a way that best suits local needs. The limited measures of this *Order* will therefore protect public safety and national security objectives in a way that is tailored to avoid any significant burdens.

We estimate that the rules adopted in this *Order* will affect a limited number of CSPs. This limited impact reflects the fact that many CSPs have already implemented the types of reasonable safeguards codified in this *Order*.[488] Specifically, we estimate that: (1) the IP physical diversity requirements will only require new reliability measures from approximately 15 entities total among operators of major IP transport facilities, IP 911 traffic aggregation facilities, and ESInet facilities; (2) the operational integrity requirement will only require new measures for approximately 25 entities; (3) the IP network monitoring requirement only require

---

[484] *NG911 Transition Order*, 39 FCC Rcd at 8220-28, paras. 182-197.
[485] *2015 911 Reliability Recon. Order*, 30 FCC Rcd at 8656-58, paras. 14-20.
[486] *CSRIC VI WG 1 Report* at 67-68; *see also NG911 Reliability FNPRM*, 40 FCC Rcd at 2690, para. 56 & n.118 (citing *CSRIC VI WG 1 Report* at 115, 122, 124, best practices 11-9-8005, 18, and 36); *id.* at 2693, para. 62 & n.132, 2695, para. 67 & n.148, 2696, para. 70 & n.152 (citing *CSRIC VI WG 1 Report* at 5, 51-52).
[487] *NG911 Transition Order*, 39 FCC Rcd at 8220-28, paras. 182-197.
[488] Staff analysis. FCC, 911RCS, https://apps2.fcc.gov/rcs911/ (analyzing 911RCS certifications from NGCS providers and ESInet operators) (last visited May 19, 2025).

new measures for approximately 25 entities; (4) the interoperability reporting requirement applicable to ESInet facilities and NGCS operators will only require new measures for approximately 25 entities; (5) the one-time upfront labor cost obligations will apply to approximately 25 entities; and (6) the certification requirement will apply to approximately 100 CSP entities.

IP Physical Diversity. We estimate a reduction in the Commission's initial estimate of IP diversity costs based on three considerations. First, since we have narrowed the major IP transport CSP category, only the largest national wireline transport providers' long-haul dedicated SIP facilities are likely to be subject to new reliability requirements. Second, because our revised IP-based physical diversity standards and streamlined certification rules do not require annual audits and tagging for each IP path to "eliminate" single points of failure, we reduce the previously proposed costs in the *NG911 Reliability FNPRM*.[489] Third, information submitted by NGCS or ESInet operators under the 2013 rules indicates that most operators already implement the level of physical diversity contemplated by the rule. According to Commission staff data, nine out of ten ESInet or NGCS providers that have filed in 911RCS already submit physical diversity reports for their paths to PSAPs, and many already use IP path diversity practices substantially similar to the IP 911 reliability framework we adopt today.[490] Accordingly, we estimate approximately 15 entities will need to obtain new transport facilities under the IP physical diversity requirements, reduced from the original 25 entities, and at lower costs than originally estimated.[491]

Up-front costs for meeting the IP path-diversity requirement involve deploying

---

[489] ESInet operators, major IP transport facilities operators, and 911 IP aggregation facilities operators will certify to having implemented IP reliability best practices sufficient to "mitigate" the risks of single points of failure. For example, Motorola's description of how it connects its geographically diverse NGCS facilities "to the PSAP via an ESInet" using multiple geographically diverse MPLS circuits with dynamic routing, and using "both MPLS and SD-WAN technologies" to ensure "efficient delivery and enhanced fault tolerance" satisfies today's IP diversity benchmark. Motorola Comments at 7. *See also NG911 Reliability FNPRM*, 40 FCC Rcd at 2720, para. 131 (estimating an annual IP diversity cost of $2.4 million).

[490] Staff analysis. FCC, 911RCS (last visited May 19, 2026), https://apps2.fcc.gov/rcs911/ (analyzing physical diversity reports for ESInet paths from NGCS facilities to PSAPs).

[491] We estimate 15 affected entities, including 10 total entities in the major IP transport and 911 IP aggregation categories, and 5 ESInet operators.

geographically redundant, load-balancing routers capable of automatic re-routing, a cost the Commission estimated as approximately $40,000 per CSP.[492] Assuming 15 entities will need to acquire new redundant routers to meet the proposed IP path diversity benchmark, the resulting one-time cost would be approximately $600,000.[493] For annual costs, to the extent 15 entities must also purchase redundant IP transport to ensure path diversity, we estimate a per-entity annual transport cost of $120,000 per CSP, resulting in annual diversity costs of $1.8 million.[494]

Some commenters raise objections to the IP diversity cost estimates in the *NG911 Reliability FNPRM*. The modifications and clarifications we adopt today to the IP path diversity benchmark, the IP path diversity certification, as well as our reducing the number of major IP transport facility CSPs by raising the threshold to OC48 or 2.5 Gbps, excluding Internet transit and TDM transport, and exempting transport providers' own originated 911 traffic as counting towards serving "two or more" OSPs, have resolved objections that these IP path diversity benchmark is too costly.[495] Specifically, we believe Lumen's estimate of $10 million in costs for two LATAs is overtaken by the multiple substantially reduced regulatory changes from the original proposals that we adopt today.[496] Given our broad reductions in burdens, we find Lumen's study does not accurately reflect the costs of our approach, despite a lack of clarity in which services Lumen was including in its study.[497] Similarly, we believe that Intrado's estimate of $75 million in labor costs, including "$250,000 per year on audit staff for 2 full-time employees" for all CSPs, is overtaken by our substantial reductions in regulatory burdens for certifications and interoperability, as well our changes to clarify that the IP path diversity benchmark does not require annual audits.[498]

---

[492] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2719, para. 129.
[493] $40,000 × 15 entities = $600,000.
[494] *See NG911 Reliability FNPRM*, 40 FCC Rcd at 2719-20, para. 130 (additional monthly cost of $3,000 IP transport to connect to third-party networks and $7,000 dedicated long-haul transport or SIP trunking). We estimate the annual IP transport costs = ($3,000 + $7,000) per month × 12 months × 15 entities = $1.8 million per year.
[495] Lumen Comments at 4; Intrado Comments at 27-29; Lumen Reply at 5-6; Verizon Comments at 10.
[496] Lumen Comments at 4.
[497] *Id.*
[498] Intrado Comments at 29-30.

We also disagree with arguments that today's diversity benchmark will significantly increase costs for OSPs.[499] We disagree with Verizon that CSP reliability measures would necessarily force more OSPs to perform services in-house.[500] Even when taking into account any increased costs of enhanced reliability measures, there are significant cost efficiencies and economies of scale in using shared transport facilities.[501] We further believe that ordinary market pressures will also keep OSP costs low, as we do not prevent OSPs from declining to hire CSPs and instead obtaining their own cloud-based, VPN, or similar public Internet transport to send their 911 traffic to in-state NG911 delivery points.[502] Because OSPs retain the ability to choose how to comply with their 911 transmission obligations, either by using a CSP, providing their own transport, or identifying non-CSP transport, we decline to clarify that reliability obligations are not the cost responsibility of OSPs. We see no clear evidence that the updates to the 911 reliability framework would necessarily increase the costs of non-CSP shared transport options.

Operational Integrity. The *NG911 Reliability FNPRM* estimated that meeting this benchmark would require investments in servers, UPS devices, and collocation space. The Commission estimated the cost of servers at approximately $5,000 each, high-end UPS devices at approximately $3,000 per unit, and any necessary diverse secondary server collocation full-rack space at approximately $700 per month.[503] Assuming that 25 entities would newly undertake these reasonable reliability measures, we estimate total one-time costs of $200,000 and recurring annual costs of $210,000.[504] Today's clarification that operators of LNGs or other mixed TDM-IP transitional facilities may implement either legacy backup power or IP

---

[499] Verizon Comments at 10-11.
[500] Verizon Comments at 11.
[501] *See NG911 Transition Order*, 39 FCC Rcd at 8199, para. 139 (observing that shared services "enable multiple small carriers to bundle their data streams and share the cost of transporting the pooled data stream to a common destination, resulting in lower overall costs than if each OSP paid for separate transport," and finding that "OSPs should be allowed to implement such reasonable cost-saving measures").
[502] 47 CFR § 9.32.
[503] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2720-21, para. 132.
[504] *Id.* (estimating one-time costs as follows: ($5,000 server cost + $3,000 UPS device) × 25 entities = $200,000; and estimating the annual cost as: $700/month × 12 months × 25 entities = $210,000 per year).

operational integrity measures as appropriate (or alternative measures) resolves commenter concerns about IP operational integrity costs.[505]

IP Network Monitoring. The *NG911 Reliability FNPRM* proposed adopting an IP network monitoring capability requirement and sought comment on the associated costs. The Commission estimated that most IP CSPs already meet this requirement and therefore would incur little to no additional compliance burden. We continue to estimate that IP network monitoring capability would involve one-time costs of $200,000 and recurring annual costs of $260,000, as originally proposed.[506] We disagree that the IP monitoring benchmark is costly due to the "spider web-like nature of IP traffic."[507] We are not requiring direct monitoring of entire IP traffic paths, only of a CSP's specified facilities along those paths—nodes, node links, and routers—as well as processing facilities like LIS, NCGS cores, etc.

Interoperability. The Commission proposed requiring CSPs to acquire interoperability capability and report annually on their efforts to become interoperable and sought comment on the associated cost estimates. The Commission's analysis assumed approximately 25 such entities nationwide and that each would incur both one-time implementation costs and ongoing annual costs because of this requirement. However, in the *Order*, we decline to adopt an interoperability benchmark, and we reduce the annual reporting requirement to a one-time report. We estimate only minimal costs for NGCS and ESInet CSPs to submit this report describing their interoperability actions and plans. Today's modifications substantially reduce the burden of the Commission's proposed interoperability benchmark and our change from an annual interoperability certification to a one-time report resolve commenter concerns that this rule could be more costly.[508] We nevertheless conservatively estimate one-time costs of $200,000 per entity and recurring annual costs of approximately $260,000 per entity under this

---

[505] Intrado Comments at 29.
[506] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2721, para. 133 (estimating one-time costs as follows: $8,000 × 25 entities = $200,000; and estimating the annual recurring cost as: (($700/month × 12 months) + $2,000 annual software license cost) × 25 entities = $260,000 per year).
[507] Intrado Comments at 29.
[508] *See* Intrado Comments at 28-30.

revised rule.

One-time Labor Costs – Software, Engineering, and Installation. As proposed in the *NG911 Reliability FNPRM*, we estimate that 25 entities are likely to spend 160 labor-hours in each of three areas—software, engineering, and installation—to meet the new IP benchmarks. No party disputed these labor estimates, and in consideration of the other rule modifications described in this section, we conclude these estimates are accurate. Applying these hour estimates to 25 entities results in a total one-time labor cost of $875,568.[509]

Attestations, Certifications, and Reporting. The attestation and streamlined certification requirements adopted here are not unduly burdensome. As clarified above, ESInet operators, major IP transport facilities operators, and IP 911 traffic aggregation facilities operators will certify only to having implemented IP network reliability best practices at a level sufficient to *mitigate* the risks associated with single points of failure, rather than to a burdensome and labor-intensive annual auditing and tagging exercise. We estimate no new incremental costs associated with the initial one-time filings applicable to CSPs under the 2013 rules, and only minimal costs for new IP CSPs to submit an initial attestation. Furthermore, CSPs will no longer file certifications annually, and we estimate only minimal annual costs from routine internal compliance inquiries and determinations of whether a material change update is needed. Accordingly, we apply the unit estimate of $48,156 per CSP per year, which represents the costs of the requirement adopted in 2013. We further assume that the rules adopted in this *Order* result in no more than 10% incremental cost and multiply it by the projected total 100 CSPs that will remain upon completion of the NG911 transition, resulting in a total average annual cost of approximately $481,560.[510]

We disagree with claims that the number of certification filers could be higher than 100 in

---

[509] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2721-22, paras. 135-36. We estimate 25 entities incur 160 hours of labor in each of three categories: $92.44 per hour for software developers, $79.68 per hour for network engineers, and $36.78 per hour for telecommunications equipment installers. This results in a total cost of $875,568.

[510] $48,156 × 10% ×100 entities = $481,560.

a post-NG911 transition environment.[511] Commenters do not substantiate this claim, and the evidence available to the Commission indicates that the number of specialized NG911 providers subject to today's rules remains small and may be consolidating further. Entities such as Sinch, Bandwidth, AT&T, Lumen, Comtech, and Intrado are increasingly providing multiple NG911 CSP functions, including NGCS, ESInet, IP 911 aggregation, major IP transport, and shared LIS service.[512] Similarly, the total number of RLECs or small providers that no longer provide covered 911 services has increased since the *NG911 Reliability FNPRM*.[513] This confirms the Commission's expectations that the NG911 transition would reduce the regulatory burden on RLECs and small entities.[514] Finally, today's modifications increasing the capacity threshold to OC48 or 2.5 Gbps for major IP transport facilities, excluding a providers' own originated 911 traffic from the "two or more" OSP threshold for major IP transport, clarifying the exclusion of Internet transit and TDM transport from the major IP transport CSP category, and specifying that only shared LIS and LNG operators are CSPs further undermines the argument that the total number of filers will be high.

Deregulatory Agenda

Today, we eliminate an excessive and burdensome annual filing requirement which imposes costs on private businesses without commensurate benefits. Our new approach to certification requires a one-time submission, to be updated only when a CSP undergoes a

---

[511] Intrado Comments at 28; Verizon Comments at 11.

[512] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2688, para. 50 & nn.105-106, 2705, para. 94 & nn.200-201, 2718, para. 126 & n.280 (A high volume of 911 IP aggregation services nationwide are provided by two companies, Sinch and Bandwidth.); *id.* at 2718, para. 126 & n.278 (AT&T is providing shared LIS services in its role as the ESInet and NGCS provider in Virginia.); Lumen Comments at 1 (stating that Lumen is an NG911 CSP, a transport provider, and an aggregator of 911 IP traffic in several states); Lumen, *Lumen® Next Generation 9-1-1 Solution*, at 2, https://assets.lumen.com/is/content/Lumen/Next_Gen_911 (describing Lumen's ESInet services) (last visited May 19, 2026); COPUC Comments at 6-7 ("A[] LIS is a function that will be built internally by an OSP or, as is more likely to be common, built by an entity such as Intrado or Comtech as a service to be provided to multiple OSPs.").

[513] CSPs are required to notify Bureau staff within 60 days after they completely cease providing all covered 911 services. 47 CFR § 9.19(d)(4). *See also PSHSB Announces Compliance Date and Instructions for Information Collection Requirement Associated with Improving 911 Reliability*, PS Docket Nos. 13-75 *et al*., Public Notice, 39 FCC Rcd 5797 (PSHSB 2024).

[514] Intrado Comments at 28; *NG911 Reliability FNPRM*, 40 FCC Rcd at 2717-18, para. 126 & n.277; *see also* Staff analysis. FCC, 911RCS (last visited May 19, 2026), https://apps2.fcc.gov/rcs911/ (analyzing the increase in former CSPs that no longer provide covered 911 services from 2024 to 2025).

material change in its network or reliability practices. In addition, we end the practice of 911 reliability certifications requiring thousands of lines of site-based data that describe each PSAP circuit and central office hosting facility, and instead require only the common-sense approach of state-level reporting. These measures will significantly cut red tape and eliminate wasteful regulatory burdens on industry, unleashing prosperity and freeing up resources that should be devoted to completing the NG911 transition as rapidly as possible.

Furthermore, the NG911 transition will dramatically decrease the burdens on industry of 911 reliability generally. The ongoing migration away from legacy 911 networks to NG911 networks means dozens of small RLECs will no longer be providing covered 911 services, such as operating selective routers or ALI/ANI databases from the local central office.[515] These RLECs will, in many instances, no longer be subject to our 911 reliability framework after the migration to NG911. In addition, the retirement of legacy TDM 911 circuits and their replacement with IP paths will eliminate the need for costly and time-consuming TDM reliability practices of annual circuit auditing and tagging. Today's *Order* will ensure that these regulatory reductions from the NG911 transition will proceed unimpeded.

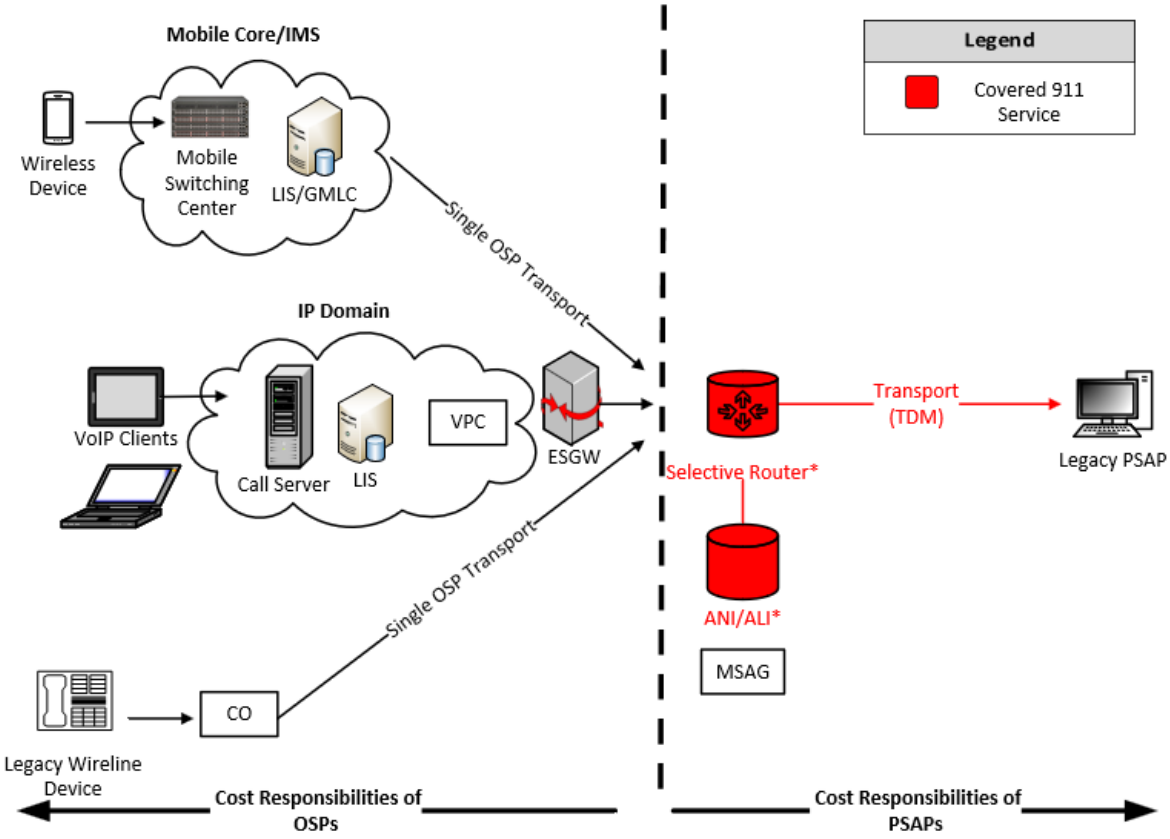
We also adopt the *NG911 Reliability FNPRM* proposal to consolidate, simplify, and streamline certain rules codified at Part 9, Subpart H of our regulations.[516] Specifically, today we achieve the following regulatory reductions: the previous §§ 9.19(c)(1) through (3) contained 25 subparts and 871 words. Today's amendments reduce §§ 9.19(c)(1) through (3) to 10 subparts and 486 words. In addition, the recordkeeping requirements at previous rule 9.19(d)(3) totaled 251 words, and today we reduce it to 107 words at § 9.20(e). We direct the Bureau to ensure these filing burdens are reduced. Collectively, all of these reductions will make our rules easier "for the average person or business to understand," reduce compliance costs, and "reduce

[515] Staff analysis. FCC, 911RCS (last visited May 19, 2026), https://apps2.fcc.gov/rcs911/ (analyzing the increase in former CSPs that no longer provide covered 911 services from 2024 to 2025).
[516] *NG911 Reliability FNPRM*, 40 FCC Rcd at 2723, para. 139.

the risk of costs of non-compliance."[517]

Diagrams – Appendix B

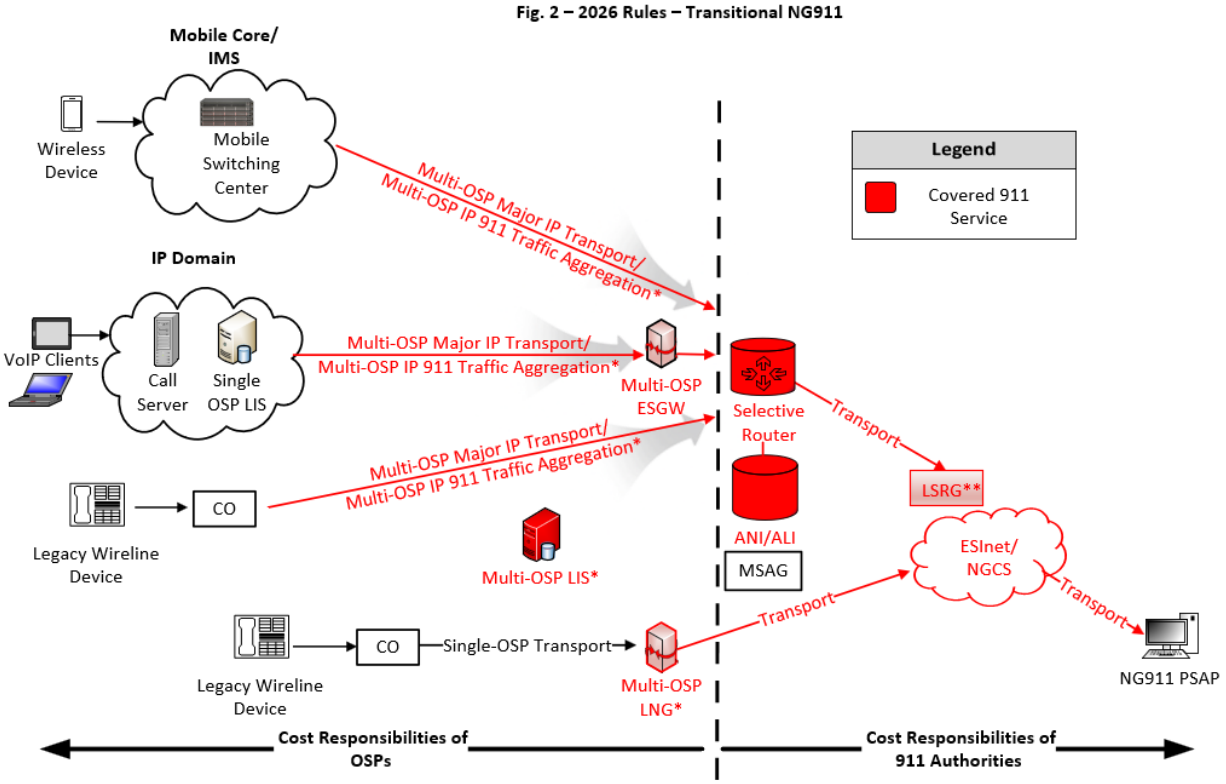
Fig. 1 – 2013 and 2026 Rules – Legacy 911 and NG911 Functional Equivalents



***Under the 2013 and 2026 rules, CSPs include entities that provide 911, E911, or NG911 capabilities such as call routing, ANI/ALI, or the functional equivalent of those capabilities directly to a PSAP and/or that operate a central office that directly serves a PSAP.**

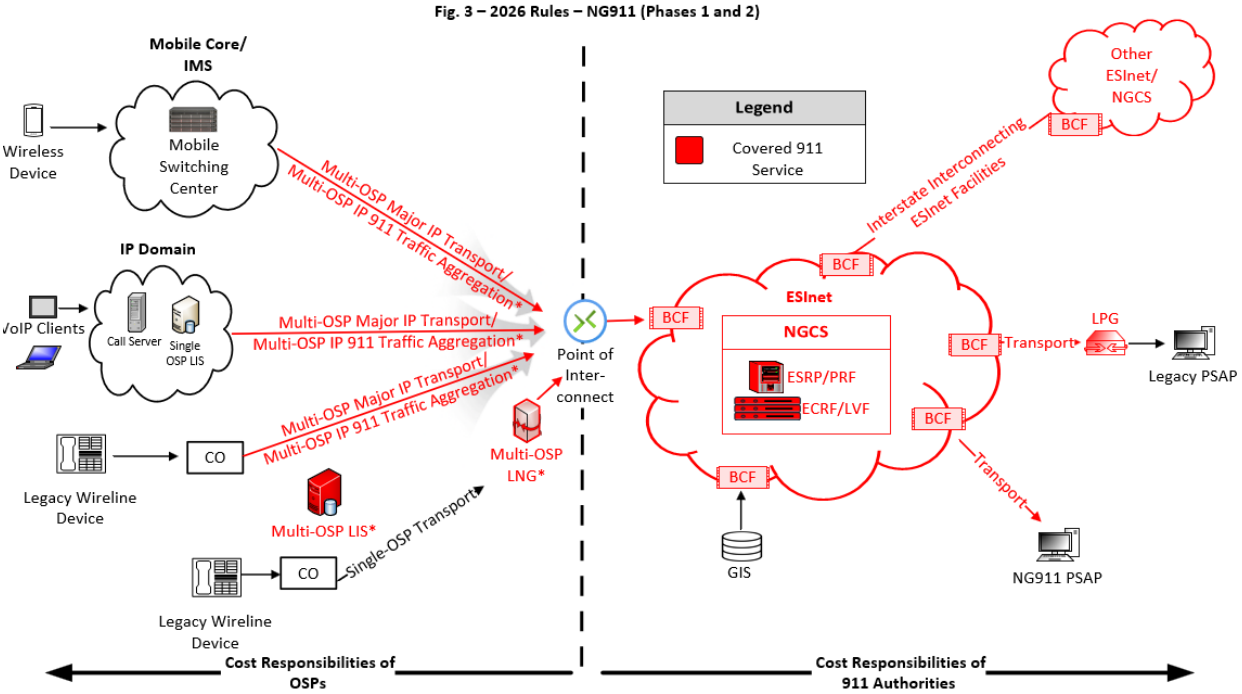
[517] Exec. Order No. 14,192, § 1, Unleashing Prosperity Through Deregulation, 90 Fed. Reg. 9065, 9065 (Feb. 6, 2025).

Fig. 2 – 2026 Rules – Transitional NG911



*OSPs may choose to use multi-OSP Major IP Transport/multi-OSP IP 911 Traffic Aggregation, LISs, or LNGs, but they are not required to do so. They may instead use single-OSP transport or multiple-OSP transport below the OC3 threshold, a single-OSP LIS, and/or a single-OSP LNG.
**A LSRG can be located at the ingress or egress of an ESInet. Here, only ingress is shown.

Fig. 3 – 2026 Rules – NG911 (Phases 1 and 2)



*OSPs may choose to use multi-OSP Major IP Transport/multi-OSP IP 911 Traffic Aggregation, LISs, or LNGs, but they are not required to do so. They may instead use single-OSP transport or multiple-OSP transport below the OC3 threshold, a single-OSP LIS, and/or a single-OSP LNG.
**A LSRG can be located at the ingress or egress of an ESInet. Here, only ingress is shown.

Procedural Matters

Regulatory Flexibility Act. The Regulatory Flexibility Act of 1980, as amended (RFA),[518] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[519] Accordingly, we have prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of rule and policy changes contained in this *Second Report and Order*.

Paperwork Reduction Act Analysis. This *Second Report and Order* may contain new or substantively modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. In this *Second Report and Order*, we have assessed the effects of these 911 reliability framework and interoperability measures will promote the safety of life and property, advance national security objectives, and empower state and local governments to manage their NG911 deployments, and that these benefits outweigh the costs that might be imposed in connection with these regulatory requirements that apply to businesses, including those with fewer than 25 employees.

OPEN Government Data Act. The OPEN Government Data Act[520] requires agencies to make "public data assets" available under an open license and as "open Government data assets," i.e., in machine-readable, open format, unencumbered by use restrictions other than intellectual

---

[518] 5 U.S.C. §§ 601-612. The RFA has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).
[519] 5 U.S.C. § 605(b).
[520] Congress enacted the OPEN Government Data Act as Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202.

property rights, and based on an open standard that is maintained by a standards organization.[521] This requirement is to be implemented "in accordance with guidance by the Director" of the OMB.[522] The term "public data asset" means "a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)]."[523] A "data asset" is "a collection of data elements or data sets that may be grouped together,"[524] and "data" is "recorded information, regardless of form or the media on which the data is recorded."[525]

Final Regulatory Flexibility Analysis

As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) incorporated an Initial Regulatory Flexibility Analysis (IRFA) in the *Facilitating Implementation of Next Generation 911 Services (NG911)*; *Improving 911 Reliability* Further Notice of Proposed Rulemaking (*NG911 Reliability FNPRM*) released in March 2025. The Commission sought written public comment on the proposals in the *NG911 Reliability FNPRM*, including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA and it (or summaries of it) will be published in the Federal Register.

A. Need for, and Objectives of, the Rules

In the *Second Report and Order*, the Commission adopts rules to ensure the resiliency, reliability, and interoperability of NG911 networks and ecosystems. With the transition to NG911, dedicated 911 networks are evolving from Time Division Multiplexing (TDM)-based architectures to Internet Protocol (IP)-based architectures, which will provide 911 Authorities

---

[521] 44 U.S.C. §§ 3502(20), (22) (definitions of "open Government data asset" and "public data asset"); *id.* § 3506(b)(6)(B) (public availability).
[522] *See* OMB Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance* (Jan. 15, 2025).
[523] 44 U.S.C. § 3502(22).
[524] *Id.* § 3502(17).
[525] *Id.* § 3502(16).

with significant new capabilities to respond to those in need of emergency assistance and to improve system resilience in comparison to legacy 911. However, for NG911 to be fully effective and accessible, it is essential that NG911 networks are designed to ensure the reliability of critical components and applications and interoperability to enable seamless transfer of 911 calls and data. The Commission's 2013 reliability rules were primarily designed for legacy 911 networks and can no longer provide adequate protection for increasingly complex NG911 call traffic. In addition, over the last decade there has been an increasing number of major, multi-state 911 service outages in parts of NG911 systems that are outside the scope of the Commission's 2013 911 reliability rules. Many of these outages likely could have been prevented or mitigated had operators implemented reliability and interoperability measures appropriate for modern, IP-based systems.

The rules are needed because the ongoing NG911 transition represents a significant change in 911 network architecture that will substantially alter the class of entities that are providing critical 911 services, requiring an update to which entities are covered 911 service providers (CSPs) under the Commission's 911 reliability rules. In legacy 911 systems, a single entity such as the local Incumbent Local Exchange Carrier (ILEC) or Rural Local Exchange Carrier (RLEC) handles most critical 911 functions for the PSAPs in its service areas, including routing to PSAPs, maintaining caller location information databases, and providing call delivery via trunk lines. In contrast, NG911 systems perform these critical functions through a variety of service providers, including Emergency Services IP Network (ESInet) operators, Next Generation Core Services (NGCS) providers, and various third-party platforms providing services to 911 originating service providers (OSPs). As the NG911 transition progresses, many smaller RLECs who are CSPs under the 2013 rules will stop providing these critical 911 functions to state and local government and retire their legacy 911 facilities, as larger NG911 service providers start performing the functions previously performed by these smaller entities.

In the *Second Report and Order*, the Commission takes targeted actions to ensure the

resiliency, reliability, and interoperability of the NG911 ecosystem and its components. First, the *Second Report and Order* designates additional categories of CSPs, the entities whose operations are essential to NG911 call delivery, and specifies that the operation of ESInets and certain NG911 routing and location core services (NGCS) are covered 911 services. Second, the *Second Report and Order* updates the benchmark measures CSPs may implement to presumptively satisfy their obligation to provide reliable 911 service with best practices appropriate to IP, and makes clear that CSPs can satisfy their reliability obligations if they adopt alternative measures requested by their state, local, territorial, or tribal 911 Authority. Third, the *Second Report and Order* requires CSPs to report their actions and plans to enable NG911 interoperability. The *Second Report and Order* revises the oversight mechanisms for compliance with the 911 reliability rules to minimize burdens on regulated entities, including by eliminating annual certifications and requiring only one-time certifications with periodic updates following material changes, along with an initial one-time filing that it is providing CSP services. In addition, the *Second Report and Order* gives 911 Authorities access to CSPs' reliability and interoperability reports, and codifies the Public Safety and Homeland Security Bureau's (Bureau's) process for investigating and remediating non-compliance.

The updated requirements in the *Second Report and Order* provide the needed transparency to state and local governments and guidance to those who operate NG911 infrastructure. The Commission believes the new rules will facilitate a more effective and reliable 911 system resulting in a national 911 service that is more accessible, reliable, and interoperable, increasing the lifesaving benefits for the public.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

Commenters Intrado and Verizon raised issues regarding the impact of the rules on small entities, although not in direct response to the IRFA. Commenters suggest that the number of certification filers could be higher than 100 in a post-NG911 transition environment, and could

include smaller entities. In the *Second Report and Order*, the Commission found these claims were not substantiated, and that the evidence indicates that the number of specialized NG911 providers subject to the Second Report and Order remains small and may be consolidating further. Similarly, the total number of RLECs or small providers who have stopped filing annual 911 reliability certifications has increased since the *NG911 Reliability FNPRM*, confirming the Commission's expectations that the NG911 transition would reduce the regulatory burden on RLECs and small entities.

Commenters also claimed that the rules could burden smaller providers if they are required to hire third parties for 911 call transport or processing that are subject to reliability requirements. Because the costs of today's item are minimal, we conclude that any costs passed on from CSPs to their OSP customers will be small. In addition, the *Second Report and Order* preserves the ability of smaller OSPs to elect not to use CSPs to deliver 911 traffic to ESInets under the NG911 framework under our rules.

C. Response to Comments by the Chief Counsel for the Small Business Administration Office of Advocacy

Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy, and also provide a detailed statement of any change made to the proposed rules as a result of those comments. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the adopted rules. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has

the same meaning as the term "small business concern" under the Small Business Act. A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA. The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.

Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions. In general, a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses. Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and are not dominant in their field. While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees. Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand. Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.

The rules adopted in the *Second Report and Order* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS) codes and corresponding SBA size standard. Where available, we also provide additional information regarding the number of potentially affected entities in the identified industries below.

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	**NAICS Code**	**SBA Size Standard**	**Total Firms**	**Total Small Firms**	**% Small Firms**
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing	334220	1,250 employees	155	136	87.74%
Semiconductor and Related Device Manufacturing	334413	1,250 employees	675	610	90.37%
Wired Telecommunications Carriers	517111	1,500 employees	3,403	3,027	88.95%
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	1,184	1,081	91.30%
Satellite Telecommunications	517410	$44 million	332	195	58.73%
All Other Telecommunications	517810	$40 million	1,673	1,007	60.19%

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data (Data as of December 2023)	**SBA Size Standard (1500 Employees)**		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Competitive Local Exchange Carriers (CLECs)	3,729	3,576	95.90
Incumbent Local Exchange Carriers (Incumbent LECs)	1,175	917	78.04
Interexchange Carriers (IXCs)	113	95	84.07
Wired Telecommunications Carriers	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)	585	498	85.13
Wireless Telephony	326	247	75.77

Table 3. Cable Entities Data

Cable Entities	**Size Standard**	**Total Firms**	**Small Firms**	**% Small Firms in Industry**
Cable System Operators (Telecom Act Standard) Small Cable Operator	Serves fewer than 498,000 subscribers, either directly or through affiliates	530	524	98.87%
Cable Companies and Systems (Rate Regulation) Small Cable Company	Serves 400,000 or fewer subscribers nationwide	530	523	98.51%
Cable Companies and Systems (Rate Regulation) Small Cable System (headends)	Serves 15,000 or fewer subscribers	4,545	3,965	87.24%

E. Description of Economic Impact and Projected Reporting, Recordkeeping and Other Compliance Requirements for Small Entities

The RFA directs agencies to describe the economic impact of adopted rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirement and

the type of professional skills necessary for preparation of the report or record.

The *Second Report and Order* may affect the reporting, recordkeeping, and/or other compliance requirements for small and other entities that provide 911 services. As explained in Section A of this FRFA, the Commission anticipates that the NG911 transition will eliminate the burdens on most small entities subject to the 2013 911 reliability rules, since most small entities designated as CSPs under those rules will likely cease providing the services of a CSP. Furthermore, eliminating annual certifications and replacing them with one-time and periodic certifications will further reduce burdens on all entities. Specifically, under the new streamlined certification process, CSPs will only be required to submit an initial compliance certification in 18 months and to update it in the event of a material change to the information covered by the certification. Also, CSPs will not be required to separately document reliability practices with respect to each individual PSAP served by the CSP, and instead may file consolidated certifications for their facilities at the network level on a per-state basis. CSPs covered by the updated rules that have not previously filed a reliability certification will also file an attestation in six months identifying themselves as covered 911 service providers. Finally, NGCS and ESInet CSPs will only file a one-time interoperability report, instead of the proposed interoperability certification to meeting benchmarks. The Commission believes that the rules in the *Second Report and Order* will ultimately not subject these small entities to increased burdens, and will not impose compliance obligations that require small entities to hire professionals. The Commission also anticipates the new requirements in the *Second Report and Order* will generally apply to larger entities.

In the *Second Report and Order,* the Commission maintains the structure of its 911 reliability framework, which requires all CSPs (including those providing NG911 services) to take reasonable measures to ensure reliability, and allows the presumptive demonstration of "reasonableness" by meeting certain "best practice" benchmarks codified in the rules and reported in a certification filing. The Commission preserves the flexibility for all CSPs to use

"alternative measures" instead of the benchmarks, and to certify to why those alternative measures are reasonable. More specifically, the Commission updates the categories of CSPs to include entities performing substantial 911 traffic aggregation, transport, and processing functions in the NG911 environment. The Commission also updates the best practice benchmarks applicable to IP and NG911 facilities and adds a "reasonable interoperability" requirement for certain CSPs. Finally, the *Second Report and Order* directs the Bureau to simplify and streamline the certification reporting process for CSPs, and to ensure 911 Authorities have access to the CSP certifications to increase state and local government oversight.

F. Discussion of Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities…including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."

The Commission believes that the limited measures taken with this *Second Report and Order* will protect public safety and national security objectives in a way that is tailored to avoid any significant burdens on small entities. Most of the rule changes were carefully considered to impose little or no costs on state and local governments or industry, including small entities. The ESInet and NGCS CSP categories are clarifications or minor modifications of the 2013 rules, and the rule updates adding CSP definitions for major IP transport facilities operators, 911 IP aggregation facilities operators, LIS operators, and LNG operators represent minimal changes to keep pace with technology evolution and ensure realization of the benefits of the *NG911 Transition Order*. The IP path diversity and IP monitoring benchmarks adopted in the *Second Report and Order* are largely codifications of the rule interpretations adopted in the *2015 911*

Reliability Recon. Order. Furthermore, both of those benchmarks and the operational integrity benchmark codify CSRIC's recommendations of NG911 reliability tools that were already available or not overly burdensome to implement based on consideration of impacts on operations and capital budgets, labor costs, and service downtimes for upgrades. Generally, the Commission believes that the addition of the interoperability report requirement represents a minor update to account for rapidly moving technology.

In addition, the Commission takes specific steps to minimize the impacts of the rules on small entities. The *Second Report and Order* substantially reduces the number of entities included in the *NG911 Reliability FNPRM's* proposed covered 911 service classes of major IP transport, IP 911 traffic aggregation, LIS operators, and LNG operators to minimize costs on industry, including small business entities. The *Second Report and Order* also narrows the major IP transport CSP category to only the largest national wireline transport providers' long-haul dedicated SIP facilities. The Commission excludes LIS and LNG operators as falling within the regulation unless they provide third-party services to more than one OSP, and further clarifies that OSPs are not subject to the CSP regulations for provisioning their own NG911 services for their own traffic, or for hiring a CSP.

The Commission's clarifications and modifications to the *NG911 Reliability FNPRM's* proposed IP diversity benchmark and the elimination of a specific interoperability benchmark will further reduce estimated costs, including on small entities. The Commission believes that the revised IP-based physical diversity standard and clarified certification rules remove any need for annual audits and tagging to "eliminate" single points of failure for each IP path, so we substantially reduce the estimated compliance labor costs for major IP transport providers, 911 IP aggregators, and ESInet operators. ESInet operators, major IP transport facilities operators, and 911 IP aggregation facilities operators will certify only to having implemented IP reliability best practices sufficient to "mitigate" the risks of single points of failure, further reducing potential impacts on small entities. The *Second Report and Order* also eliminates the

requirement that CSPs file annual compliance certifications and adopts a streamlined filing process in which CSPs will submit a one-time reliability certification subject to updates only in the event of material changes. In addition, the *Second Report and Order* provides for an 18-month transition period before CSPs must file initial reliability certifications in conformance with the new rules, and during which CSPs will not be required to comply with the new reliability benchmarks. These steps will minimize the regulatory impacts on all CSPs including small entities.

The Commission preserves flexibility for all CSPs to implement alternative reliability practices based on engineering decisions in the field, and in a way that best suits local needs – including alternative measures agreed upon between a CSP and a 911 Authority. The Commission also limits the NGCS CSPs to those that that provide 911 routing and caller location services directly by contract to 911 Authorities, preserving flexibility for state and local governments in their service contracts with NGCS providers, and preserving local decision-making on whether state or local governments will enter agreements with NGCS providers. Accordingly, state and local governments will not be constrained by federal regulations that would automatically impose costs on any private entity that does business with state and local government, which could impose undue burdens on the smallest local government entities such as PSAPs. By preserving flexibility in state and local government NG911 deployments, the Commission ensures that related cost decisions involving small government entities will be made at the state and local level, not by the Commission.

The *Second Report and Order* also eliminates annual filing requirements, replacing them with a one-time certification that only must be updated periodically after a material change, plus a one-time filing to confirm CSP status. The *Second Report and Order* further directs the Bureau to streamline the certification form by allowing CSPs to report their compliance on a statewide basis, rather than the prior process where CSPs had to list each facility separately.

G. Report to Congress

The Commission will send a copy of the *Second Report and Order*, including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the *Second Report and Order*, including this Final Regulatory Flexibility Analysis, to the Chief Counsel for the SBA Office of Advocacy and will publish a copy of the *Second Report and Order*, and this Final Regulatory Flexibility Analysis (or summaries thereof) in the Federal Register.

Ordering Clauses

Accordingly, *it is ordered*, pursuant to sections 1, 2, 4(i), 201, 214, 225, 251(e), 301, 303, 316, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 201, 214, 225, 251(e), 301, 303, 316, 332; the Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, as amended, 47 U.S.C. 615 note, 615, 615a, 615a-1, 615b; and section 106 of the Twenty-First Century Communications and Video Accessibility Act of 2010, Pub. L. No. 111-260, 47 U.S.C. § 615c, that this *Second Report and Order is adopted*.[526]

It is further ordered that the Commission's rules are amended as set forth in Appendix A of the *Second Report and Order* and *will become effective* 30 days after publication in the Federal Register. Compliance with certain information collection provisions of 47 CFR 9.20 will not be required until after any review by the Office of Management and Budget has concluded and the Public Safety and Homeland Security Bureau announces the compliance date by subsequent Public Notice.

It is further ordered that the Commission's Office of the Secretary *shall send* a copy of this *Second Report and Order*, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

It is further ordered that the Office of the Managing Director, Performance Program

[526] Pursuant to Executive Order 14215, 90 Fed. Reg. 10447 (Feb. 24, 2025), this regulatory action has been determined to be not significant under Executive Order 12866, 58 Fed. Reg. 51735 (Oct. 4, 1993).

Management, SHALL SEND a copy of this *Second Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, 5 U.S.C. 801(a)(1)(A).

List of Subjects

47 CFR Part 0

Authority delegations (Government agencies), Classified information, Communications, Communications common carriers, Equal access to justice, Freedom of information, Government publications, Infants and children, Investigations, Organization and functions (Government agencies), Penalties, Postal Service, Privacy, Reporting and recordkeeping requirements, Sunshine Act, Telecommunications.

47 CFR Part 9

Communications, Communications common carriers, Communications equipment, Internet, Radio, Reporting and recordkeeping requirements, Satellites, Security measures, Telecommunications, Telephone.

Federal Communications Commission.

Marlene Dortch,
Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 0 and 9 as follows:

PART 0 – COMMISSION ORGANIZATION

1. The authority citation for part 0 continues to read as follows:

Authority: 47 U.S.C. 151, 154(i), 154(j), 155, 225, 409, and 1754, unless otherwise noted.

2. Amend § 0.392 by revising paragraph (j) to read as follows:

§ 0.392 Authority delegated.

* * * * *

(j) The Chief of the Public Safety and Homeland Security Bureau is delegated authority to administer the communications resiliency, redundancy, interoperability, and reliability rules and policies contained in part 9, subpart H of this chapter, develop and revise forms and procedures as may be required for the administration of part 9, subpart H of this chapter, review attestations, certifications, and reports filed in connection therewith, and request relevant documents and information and order remedial action on a case-by-case basis to ensure the reliability and interoperability of 911 service in accordance with such rules and policies.

* * * * *

3. Amend § 0.457 by revising paragraph (d)(1)(viii) to read as follows:

§ 0.457 Records not routinely available for public inspection.

* * * * *

(d) * * *

(1) * * *

(viii) Information submitted in connection with 911 reliability certifications and 911 interoperability reports pursuant to part 9, subpart H of this chapter that consists of non-public information or descriptions of networks or facilities, compliance plans, or supplemental information requested by the Commission with respect to such certifications or reports. This

information is available to 911 Authorities upon request subject to the conditions in part 9, subpart H of this chapter.

* * * * *

PART 9 – 911 REQUIREMENTS

4. The authority citation for part 9 continues to read as follows:

Authority: 47 U.S.C. 151-154, 152(a), 155(c), 157, 160, 201, 202, 208, 210, 214, 218, 219, 222, 225, 251(e), 255, 301, 302, 303, 307, 308, 309, 310, 316, 319, 332, 403, 405, 605, 610, 615, 615 note, 615a, 615b, 615c, 615a-1, 616, 620, 621, 623, 623 note, 721, and 1471, and Section 902 of Title IX, Division FF, Pub. L. 116-260, 134 Stat. 1182, unless otherwise noted.

5. Revise the heading of subpart H to read as follows:

Subpart H – Resiliency, Redundancy, Interoperability, and Reliability of 911 Communications

6. Revise and republish § 9.19 to read as follows:

§ 9.19 Provision of reliable 911 service.

(a) *Definitions*. Terms in this section and § 9.20 have the meanings set forth in §§ 9.3 and 9.28 and as follows:

(1) *Monitoring aggregation point*. A point at which network monitoring data for a 911 service area is collected and routed to a network operations center (NOC) or other location for monitoring and analyzing network status and performance.

(2) *Certification*. An attestation by a certifying official, under penalty of perjury, that a covered 911 service provider:

(i) Has satisfied the obligations of paragraph (c) of this section and § 9.20(a);

(ii) Has adequate internal controls to bring material information regarding network architecture, operations, and maintenance to the certifying official's attention; and

(iii) Has made the certifying official aware of all material information reasonably necessary to complete the certification.

(3) *Certifying official*. A corporate officer of a covered 911 service provider with supervisory and budgetary authority over network operations in all relevant service areas.

(4) *Covered 911 service provider*. (i) Any entity that provides 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:

(A) The provision of 911, E911, or NG911 capabilities such as 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), statewide default answering point, or appropriate local emergency authority as defined in § 9.3.

(B) The operation of one or more central offices that directly serve a PSAP. For purposes of this section, a central office directly serves a PSAP if it hosts a selective router or ALI/ANI database, provides equivalent NG911 capabilities, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP.

(C) The provision of 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.

(D) The operation of an ESInet or legacy PSAP gateway (LPG).

(E) The operation of a Location Information Server (LIS) or equivalent IP 911 location database that provides service to two or more originating service providers (OSPs).

(F) The operation of 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.

(G) The operation of a major IP transport facility.

(H) The operation of an IP 911 traffic aggregation facility.

(I) The operation of interstate interconnecting ESInet facilities.

(J) For purposes of the requirement in § 4.9(h) of this chapter to notify 911 special facilities about outages that potentially affect them, only entities described in paragraphs (a)(4)(i)(A) through (D) of this section are "covered 911 service providers."

(ii) The term "covered 911 service provider" shall not include any entity that:

(A) Constitutes a PSAP, 911 Authority, or other governmental authority to the extent that it provides 911, E911, or NG911 capabilities; or

(B) Offers the capability to originate 911 calls where another service provider delivers those calls and associated number or location information to the appropriate 911 Authority.

(5) *Covered 911 circuits and paths*—(i) *Legacy covered 911 circuits.* 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, including all equipment in the serving central office necessary for the delivery of 911 calls to the PSAP. 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.

(ii) *IP covered 911 paths.* Paths carrying IP communications that:

(A) 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, including all equipment associated with a covered 911 service necessary for the delivery of 911 traffic to the PSAP, such as any trunks, circuits, or paths to and from NGCS facilities and the ESInet transmission network necessary for routing and caller location information to the PSAP(s), and any intermediate paths in the chains of delivery;

(B) Transport 911 traffic via major IP transport facilities for ultimate delivery at an NG911 Delivery Point or equivalent ESInet point of interconnection, including any intermediate paths in the chain of delivery; or

(C) Transport 911 traffic via IP 911 traffic aggregation facilities for ultimate delivery at an NG911 Delivery Point or equivalent ESInet point of interconnection, including any interconnecting paths between ESInets, and including any intermediate paths in the chain of delivery.

(6) *Diversity audit*. A periodic analysis of the geographic routing of network components to determine whether they are physically diverse. Diversity audits may be performed through manual or automated means, or through a review of paper or electronic records, as long as they reflect whether covered 911 circuits and paths are physically diverse.

(7) *Monitoring links*. Facilities that collect and transmit network monitoring data to a NOC or other location for monitoring and analyzing network status and performance.

(8) *Physically diverse*. Circuits or paths are physically diverse if they provide more than one physical route between end points with no common points where a single failure at that point would cause both circuits or paths to fail. Circuits or paths that share a common segment such as a fiber-optic cable or circuit board are not physically diverse even if they are logically diverse for purposes of transmitting data. IP routers, transport nodes, and node links create physical diversity if these elements are redundant, geographically distributed, load balanced, and capable of automatic failover and rerouting to redundant elements sufficient to reasonably mitigate the risks of single points of failure.

(9) *Tagging*. An inventory management process whereby legacy covered 911 circuits are labeled in circuit inventory databases to make it less likely that circuit rearrangements will compromise diversity. A covered 911 service provider may use any system it wishes to tag legacy covered 911 circuits so long as it tracks whether those facilities are physically diverse and identifies changes that would compromise such diversity.

(10) *Geographically distributed*. 911 network architecture is geographically distributed if 911 traffic can be delivered through more than one covered 911 facility in different geographic locations in different physical facilities.

(11) *Load balanced*. 911 network architecture is load balanced if call volume is dynamically distributed among multiple active databases or call processing facilities to accommodate changes in traffic volume.

(12) *Major IP transport facility*. Dedicated SIP facilities that include voice and text transport meeting or exceeding Optical Carrier 48 (OC48) / 2.5 Gbps in capacity that collect and/or transmit IP 911 traffic mixed with non-911 traffic, originated from two or more OSPs and transported over interstate routes, for ultimate transport and delivery to an NG911 Delivery Point or equivalent ESInet point of interconnection. Any 911 traffic originated on the facility provider's network is not considered for purposes of determining whether a provider is serving two or more OSPs.

(13) *IP 911 traffic aggregation facility*. Facilities that collect and segregate IP 911 traffic from non-911 traffic for two or more OSPs, or transport such 911-only traffic for ultimate delivery to an NG911 Delivery Point or equivalent ESInet point of interconnection. Any 911 traffic originated on the facility provider's network is not considered for purposes of determining whether a provider is serving two or more OSPs.

(14) *NGCS location facilities*. NG911 IP facilities connected to an ESInet that enable the real-time provision of 911 caller location information to the PSAPs, including but not limited to the Emergency Call Routing Function (ECRF), the Location Validation Function (LVF), and successor technologies.

(15) *NGCS routing facilities*. NG911 IP facilities connected to an ESInet that enable the real-time routing, delivery, or transfer of 911 traffic to PSAPs along with callback information and other associated data, including but not limited to the Emergency Services Routing Proxy (ESRP), the Policy Routing Function (PRF), and successor technologies.

(16) *Interstate interconnecting ESInet facilities*. Interstate facilities that transport IP 911 traffic from an ESInet for ultimate delivery to another ESInet, including facilities designated for intermittent, contingent, or backup exchange of IP 911 traffic between ESInets.

(17) *Interoperability standards testing*. Testing of covered 911 services and covered 911 circuits and paths to determine whether an NG911 interoperability solution conforms to a relevant commonly accepted standard.

(18) *Interoperability conformance testing*. Testing conducted between two or more NG911 covered 911 service providers in different states that validate the interoperable exchange of information.

(19) *Interoperability*. 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.

(b) *Provision of reliable 911 service*. All covered 911 service providers shall take reasonable measures to provide reliable 911 service that ensures physical diversity, operational integrity, and network monitoring for their covered 911 facilities. Performance of the elements of the certification set forth in paragraphs (c)(1) through (3) of this section shall be deemed to satisfy the requirements of this paragraph (b). If a covered 911 service provider cannot certify that it has performed a given element, the Commission may determine that such provider nevertheless satisfies the requirements of this paragraph (b) based upon a showing that it is taking alternative measures with respect to that element that are reasonably sufficient to mitigate the risk of failure, or that one or more certification elements are not applicable to its network.

(c) *911 reliability benchmarks*—(1) *Physical diversity*. A covered 911 service provider shall certify that all IP covered 911 paths and legacy covered 911 circuits in its network are physically diverse as defined in paragraph (a)(8) of this section.

(i) For IP covered 911 paths, covered 911 service providers may satisfy this physical diversity benchmark by implementing automatic rerouting capabilities, load balancing, and geographically-distributed routing facilities, transport nodes, and node links sufficient to reasonably mitigate the risks of single points of failure. Covered 911 service providers may use 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.

(ii) For legacy covered 911 circuits, covered 911 service providers may satisfy this physical diversity benchmark by conducting yearly diversity audits and certifying that all of the legacy covered 911 circuits in its network are tagged and are physically diverse such that no network or facility element constitutes a single point of failure.

(2) *Operational integrity*. A covered 911 service provider shall certify whether its central offices hosting selective routers, ALI/ANI, or functioning as the last central office serving a PSAP, or its LNG, LIS, LSRG, ESGW, LPG, or NGCS functional elements covered by paragraph (a)(4)(i) of this section in its network achieve operational integrity. Transitional elements for TDM-IP conversion, such as the LSRG or LPG, may certify to either paragraph (c)(2)(i) or (ii) of this section, in the latter case with 24 hours of backup power.

(i) LNGs, LISs, LSRGs, ESGWs, LPGs, and NGCS facilities covered by paragraph (a)(4)(i) of this section achieve operational integrity if they have the capability to ensure continuity of services via an uninterruptible and continuous power supply and automatic switchover to geographically diverse backup facilities sufficient to prevent service disruption.

(ii) For central offices hosting selective routers, ALI/ANI, or functioning as the last central office serving a PSAP, covered 911 service providers satisfy this operational integrity benchmark by implementing backup power facilities for covered legacy 911 central office facilities for at least 24 hours at full office load if the central office directly serves a PSAP, or, for at least 72 hours at full office load if the central office hosts a selective router, including all

equipment design, proper installation, necessary testing, and equipment maintenance to ensure the automatic and independent function of backup power facilities.

(3) *Network monitoring*. A covered 911 service provider shall certify whether it uses physically diverse monitoring to detect outages and disruptions in its covered facilities.

(i) Using geographically distributed automatic disruption detection and alarm systems to monitor IP covered facilities, including the IP routers, transport nodes, and node links used to make covered 911 circuits and paths physically diverse, constitutes physically diverse monitoring.

(ii) For non-IP covered facilities, maintaining and annually auditing physically diverse monitoring aggregation points, monitoring links, and NOCs constitutes physically diverse monitoring.

(d) *Compliance date*. For covered 911 service providers described at paragraphs (a)(4)(i)(E) through (I) of this section, compliance with the reliability requirement at paragraph (b) of this section will not be required until 18 months from the date of issuance of a Public Notice announcing a compliance date for those paragraphs. For all covered 911 service providers, compliance with the benchmarks at paragraphs (c)(1)(i), (c)(2)(i), and (c)(3)(i) of this section will not be required until 18 months from the date of issuance of a Public Notice announcing a compliance date for those paragraphs.

7. Add § 9.20 to read as follows:

§ 9.20 911 Reliability certifications; interoperability reporting; cessation notifications.

(a) *911 reliability filings*—(1) *Attestation*. (i) Within six months of a Public Notice announcing a compliance date for this paragraph (a)(1) and filing guidelines, any covered 911 service provider that has not previously filed a reliability certification shall submit to the Commission an attestation identifying itself as a covered 911 service provider. Attestations will not be deemed confidential.

(ii) Any new covered 911 service provider that begins service for the first time after the date in paragraph (a)(1)(i) of this section shall submit an attestation when it begins service.

(2) *Certification*—(i) *Initial certification*. Within 18 months of a Public Notice announcing a compliance date for this paragraph (a)(2) and filing guidelines, a certifying official of each covered 911 service provider shall submit a certification to the Commission that addresses the elements of reliability listed in § 9.19(c)(1) through (3).

(ii) *Updates covering material changes.* A covered 911 service provider must exercise reasonable judgement in determining whether there is a material change to its ownership structure, networks, facilities, operations, or reliability practices that renders its previous certification no longer accurate and file an updated certification within 90 days of discovery of such a material change, unless:

(A) The cause of the change is remedied within the applicable update period;

(B) The change reflects incremental conformance with the reliability elements in § 9.19(c)(1) through (3), rather than reliance on alternative measures, for less than 50 percent of its covered 911 services, circuits, and paths; or

(C) The change to a covered 911 service provider's ownership structure is *pro forma* in nature.

(iii) *Non-conforming facilities and services.* If a covered 911 service provider does not conform with the elements of reliability listed in § 9.19(c)(1) through (3), it must include in its certification with respect to each of its non-conforming covered 911 circuits or paths and covered 911 services whether:

(A) The covered 911 service provider has taken alternative measures to mitigate the risks of lack of physical diversity, operational integrity, or network monitoring; or

(B) The physical diversity, operational integrity, or network monitoring benchmark is not applicable to the covered 911 service provider.

(iv) Covered 911 service providers are required to answer additional questions about covered 911 circuits and paths and covered 911 services as directed by the Public Safety and Homeland Security Bureau.

(b) *911 interoperability reports*. (1) Each NGCS and ESInet covered 911 service provider defined in § 9.19(a)(4)(i)(C) or (D) shall submit a one-time report to the Commission describing its specific actions and plans to enable NG911 interoperability consistent with § 9.19(a)(19) within 18 months of a Public Notice announcing a compliance date for this paragraph and filing guidelines.

(2) NGCS and ESInet covered 911 service providers defined in § 9.19(a)(4)(i)(C) or (D) are required to answer additional questions about covered 911 circuits and paths and covered 911 services as directed by the Public Safety and Homeland Security Bureau.

(c) *Confidential treatment of certifications and reports.* (1) The fact of filing or not filing 911 reliability certifications and 911 interoperability reports shall not be treated as confidential.

(2) Information submitted with such certifications and reports shall be 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 with respect to a certification.

(d) *911 Authority access to certifications and reports*. (1) Following the compliance date for initial certifications and reports, a statewide, territorial, or tribal 911 Authority may request that covered 911 service providers produce copies of their 911 reliability certifications and interoperability reports to the extent they pertain to covered 911 services or covered 911 circuits and paths located within or providing services to the 911 Authority's jurisdiction.

(2) Covered 911 service providers must provide the requested certifications or reports within 14 days of a request. Covered 911 service providers may omit or redact information relating to portions of their networks or facilities that are not located within and do not provide service to the requesting 911 Authority's jurisdiction. Covered 911 service providers may

condition the granting of such requests on the 911 Authority's execution of a confidentiality agreement under terms not more restrictive than those set forth in § 4.2 of this chapter and in related guidance, instructions, and forms published by the Commission.

(3) To the extent the Public Safety and Homeland Security Bureau provides statewide, territorial, or tribal 911 Authorities with, or grants them access to, 911 reliability certifications and interoperability reports, it shall do so in accordance with relevant confidentiality terms and conditions pursuant to which it provides access to NORS data under § 4.2 of this chapter and related guidance, instructions, and forms published by the Commission.

(e) *Record retention*. A covered 911 service provider shall retain records supporting its responses in 911 reliability certifications and interoperability reports for two years from the date of filing, and shall make such records available to the Commission upon request. To the extent that a covered 911 service provider maintains records in electronic format, records supporting such a certification or report shall be maintained and supplied in an electronic format. Such records shall include, at a minimum, any audit records, internal reports concerning reliability and interoperability compliance, records of action to achieve reliability and interoperability compliance, and testing and maintenance of reliability and interoperability measures and technology.

(f) *Covered service cessation notices*. Covered 911 service providers that cease covered operations under § 9.19 must notify the Commission by filing a notification under penalty of perjury no later than 60 days after the cessation of service.

(g) *Remedial action orders and procedures*. When acting pursuant to authority delegated under § 0.392(j) of this chapter to order remedial actions, the Chief of the Public Safety and Homeland Security Bureau (Bureau Chief) will carry out restricted non-public proceedings with parties regulated under this subpart as follows:

(1) *Notice.* If certifications or other information available to the Commission indicate that a covered 911 service provider may not be taking reasonable measures to provide reliable 911

service, the Bureau Chief may issue and electronically serve upon the covered 911 service provider a notice that describes any apparent deficiencies and proposes remedial actions. The notice may include requests for relevant documents and information.

(2) *Response.* A covered 911 service provider may submit a written response to a notice within 30 days of service of such notice and shall provide any requested documents and information by such date. Service shall be made as directed by the Bureau.

(3) *Order.* At any time after the 30th day following service of a notice, the Bureau Chief may issue and serve upon the covered 911 service provider an order setting forth its findings as to such deficiencies and specifying the actions that the covered 911 service provider is required to take to mitigate the deficiencies. The order may specify deadlines by which the covered 911 service provider must complete the required actions and may identify information that the provider must submit to demonstrate its compliance with the order.

(4) *Notice to 911 Authorities*. The covered 911 service provider shall deliver a copy of the order promptly to the 911 Authority for each jurisdiction in which its actions have been found deficient or in which it has been directed to take remediating actions.

(h) *Compliance date*. This section may contain information collection and recordkeeping requirements that require review by the Office of Management and Budget. Compliance with new information collection and recordkeeping requirements will not be required until this paragraph (h) is removed or contains a compliance date.

[FR Doc. 2026-13998 Filed: 7/9/2026 8:45 am; Publication Date: 7/10/2026]