FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0 and 9

[PS Docket Nos. 21–479 and 13–75, FCC 25–21; FR ID 295635]

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

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (the FCC or Commission) proposes rules that would help 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 safeguard the reliability of critical components and support the interoperability needed to seamlessly transfer 911 calls and data from one network to another. When the Commission first adopted 911 reliability rules in 2013, the transition to NG911 was in its very early stages. Since then, many state and local 911 Authorities have made significant progress in deploying NG911 capabilities in their jurisdictions. This Further Notice of Proposed Rulemaking (FNPRM) is the next step in fulfilling the Commission's commitment to facilitate the NG911 transition and to ensure that the transition does not inadvertently create vulnerabilities in the nation's critical public safety networks. The FNPRM proposes to update the definition of ''covered 911 service provider'' in the Commission's existing 911 reliability rules to ensure that the rules apply to service providers that control or operate critical pathways and components in NG911 networks. It also proposes to update the reliability standards for providers of critical NG911 functions to ensure the reliable delivery of 911 traffic to NG911 delivery points, and proposes to establish NG911 interoperability requirements for interstate transfer of 911 traffic between Emergency Services IP Networks (ESInets). In addition, the FNPRM proposes to modify the certification and oversight mechanisms in the current 911 reliability rules to improve reliability and interoperability in NG911 systems while minimizing burdens on service providers, and proposes to empower state and local 911 Authorities to obtain reliability and interoperability certifications directly from covered 911 service providers.

DATES: Comments are due on or before July 21, 2025, and reply comments are due on or before August 18, 2025.

ADDRESSES: Pursuant to §§ 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). See Electronic Filing of Documents in Rulemaking Proceedings, 63 FR 24121 (1998), *https://www.govinfo.gov/content/pkg/FR-1998-05-01/pdf/98-10310.pdf.* You may submit comments, identified by PS Docket Nos. 21–479 and 13–75, by any of the following methods:

- *Electronic Filers:* Comments may be filed electronically using the internet by accessing the ECFS: *https://www.fcc.gov/ecfs.*
- *Paper Filers:* Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. All filings must be addressed to the Secretary, Federal Communications Commission.
- Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.
- *People With Disabilities:* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530.

FOR FURTHER INFORMATION CONTACT: Chris Fedeli, *Christopher.Fedeli@fcc.gov* or 202–418–1514, or Daniel Spurlock, *Daniel.Spurlock@fcc.gov* or 202–418–0212, Attorney-Advisors, of the Public Safety and Homeland Security Bureau, Policy and Licensing Division.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Further Notice of Proposed Rulemaking (FNPRM), in PS Docket Nos. 21–479 and 13–75, FCC 25–21, adopted on March 27, 2025, and released on March 28, 2025. The full text of this document is available at *https://docs.fcc.gov/public/attachments/FCC-25-21A1.pdf.*

Ex Parte Presentations—Permit-But-Disclose. The Commission will treat this proceeding as a ''permit-but-disclose'' proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.,* .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

Providing Accountability Through Transparency Act. Consistent with the Providing Accountability Through Transparency Act, Public Law 118–9, a summary of this FNPRM will be available on *https://www.fcc.gov/proposed-rulemakings.*

Synopsis

Introduction

In this Further Notice of Proposed Rulemaking (FNPRM), we propose to update existing Commission rules to ensure the resiliency, reliability, interoperability, and accessibility of Next Generation 911 (NG911) networks. 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 state and local 911 authorities with significant new capabilities to respond to those in need of emergency assistance and to improve system resilience in comparison to legacy 911. These new capabilities include multimedia NG911 calls that allow the transmission of texts, photos, videos, and data, which persons with disabilities depend on for full and equal access to emergency services. 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.

Today, we propose certain reliability and interoperability requirements that would apply to ''covered 911 service providers'' (CSPs), the providers that support essential functions within 911 networks such as call routing and automatic caller location, with particular emphasis on entities that provide these capabilities in the NG911 environment.[1] Our proposals build on the 911 reliability rules that the Commission adopted in 2013, which require CSPs to take measures to provide reliable 911 service to Public Safety Answering Points (PSAPs) with respect to circuit diversity, central-office backup power, and diverse network monitoring.[2] We propose to modify and update these rules to keep pace with the ongoing transition to NG911, improve NG911 network reliability and resilience, reduce the risk of outages, and ensure accessibility to the life-saving improvements that NG911 is uniquely capable of delivering. We also propose to adopt rules that would require Emergency Services IP Network (ESInet) providers to support interoperability in the interstate transfer of 911 calls and data, which will strengthen the ability of state and local 911 Authorities to ensure continued access to NG911 services during major emergencies by deploying resources in support of one another.[3]

It is particularly important that we take action on these issues now. When the Commission adopted the current 911 reliability rules in 2013, the transition to NG911 was in its very early stages. However, as the Commission observed in its July 2024 *NG911 Transition Order,* the NG911 transition has now progressed to the point that most states have invested in NG911 technology, and many states and local jurisdictions have operating ESInets.[4] Moreover, many public safety commenters in the *NG911 Transition* proceeding expressed strong support for the Commission taking further action to strengthen NG911 reliability, interoperability, and accessibility. Finally, while NG911 has inherent reliability and accessibility advantages over legacy 911, our experience with recent outages affecting 911 suggests that some critical elements of NG911 networks may not be adequately covered by our existing 911 reliability rules. To address these issues, we propose and seek comment on the following measures:

- *Covered 911 Service Providers.* First, we propose to update the definition of ''covered service provider'' in the Commission's existing 911 reliability rules to specify how the rules apply to service providers that control or operate critical pathways and components of NG911 networks.
  - The current CSP definition focuses on providers of certain network facilities and capabilities that are specific to legacy 911 systems and states that the rules also apply to their ''functional equivalents'' in the NG911 environment. We propose to specify that certain critical NG911 facilities and capabilities (*e.g.,* Location Validation Functions (LVFs), Geographic Information Systems (GISs), Emergency Call Routing Functions (ECRFs), Emergency Services Routing Proxies (ESRPs), and Policy Routing Functions (PRFs)) are among the functional equivalents referred to in the current rule and that providers of these capabilities therefore fall within the definition of CSPs.
  - We also propose to expand the CSP definition to encompass the following types of providers of critical connectivity in the NG911 environment: (1) operators of Location Information Servers (LISs) or equivalent IP 911 location databases; (2) operators of Legacy Network Gateways (LNGs); (3) operators of interstate Major Transport Facilities that meet or exceed Optical Carrier 3 (OC3) capacity and carry 911 traffic from multiple OSPs for ultimate delivery to NG911 Delivery Points or ESInets; (4) operators of IP Traffic Aggregation Facilities that carry segregated 911 traffic from multiple OSPs towards ultimate transmission to an NG911 Delivery Point or ESInet; and (5) operators of interstate interconnecting facilities between ESInets.[5]
- *Reliability Standards.* Second, we propose to update the reasonable reliability standards that providers of critical NG911 functions must employ to ensure the reliable delivery of 911 traffic to NG911 delivery points. We believe such action is needed to ensure the reliability of critical transport, aggregation, and data facilities in the NG911 ecosystem at the interstate and national level and the accessibility of NG911 services.

[1] *See* 47 CFR 9.19(a)(4) (defining a CSP as any entity that (A) ''[p]rovides 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 [PSAP] . . . ; and/or (B) [o]perates one or more central offices that directly serve a PSAP'').

[2] *See* 47 CFR 9.19; *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, 17477–78, paras. 2–5 (2013), 79 FR 3123 (Jan. 17. 2014) (*911 Reliability Order*); FCC Public Safety and Homeland Security Bureau, Impact of the June 2012 Derecho On Communications Networks and Services: Report and Recommendations at 1–2 (2013) (*Derecho Report*), *http://www.fcc.gov/document/derecho-report-and-recommendations.* PSAP refers to ''[a]n answering point that has been designated to receive 911 calls and route them to emergency services personnel.'' 47 CFR 9.3.

[3] An ESInet is ''[a]n internet Protocol (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. 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.'' *Id.*

[4] *Facilitating Implementation of Next Generation 911 Services (NG911); Location-Based Routing for Wireless 911 Calls,* PS Docket Nos. 21–479 and 18–64, Report and Order, FCC 24–78, 2024 WL 3507091 at *12, para. 29 (Jul. 19, 2024), 89 FR 78066 (Oct. 17, 2024) (*NG911 Transition Order*).

[5] OSPs are ''[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 this part.'' 47 CFR 9.28. The term ''911 traffic'' means ''[t]ransmissions consisting of all 911 calls (as defined in §§ 9.3, 9.11(b)(2)(ii)(A), 9.14(d)(2)(iii)(A), and 9.14(e)(2)(ii)(A)) and/or 911 text messages (as defined in § 9.10(q)(9)), as well as information about calling parties' locations and originating telephone numbers and routing information transmitted with the calls and/or text messages.'' *Id.*

• *Interoperability.* Third, we propose to establish NG911 interoperability requirements for interstate transfer of 911 traffic between ESInets to optimize PSAP call transfer capabilities during service disruptions. We seek to ensure that PSAPs can transfer calls to nearby PSAPs located across state borders with minimal need for the traffic to be retranslated or reformatted in order for such transfers to occur. We further propose to harmonize this action with our current 911 reliability certification rules by adding an interoperability certification to the rules. We also seek updated information on interstate interoperability by type of service, with particular emphasis on services used by consumers, including those with accessibility needs.

• *Oversight.* Finally, we propose to modify the certification and oversight mechanisms in our 911 reliability rules to improve implementation of reliability and interoperability in NG911 systems. Additionally, we propose to enable state and local 911 Authorities to obtain reliability and interoperability certifications directly from CSPs, so that 911 Authorities can more easily exercise their existing authority to address reliability, interoperability, and accessibility needs within their jurisdictions.

Together, these proposals are intended to improve transparency and accountability during the NG911 transition and help ensure that the nation's 911 system functions effectively and reliably. We believe that these proposals will make the nation's 911 service more accessible, reliable and interoperable, while striking an appropriate balance between costs and benefits of such regulation. We seek comment on the tentative conclusions, proposals, and analyses set forth in this FNPRM, as well as on any alternative approaches.

Background

A. 911 Reliability Framework

The Commission adopted certain, specific 911 reliability rules for ''covered 911 service providers'' or CSPs in 2013 following the devastating impact on 911 services of the June 2012 mid-Atlantic derecho storm.[6] In the 2013 911 Reliability Order, the Commission determined that the reliability, resiliency, and availability of 911 service could be improved through implementation of network reliability practices and other sound engineering principles, and it accordingly adopted 911 reliability certification rules for CSPs.[7] CSPs are entities that provide 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 PSAP, statewide default answering point, or appropriate local emergency authority.[8] The rules mandate that all CSPs ''shall take reasonable measures to provide reliable 911 service with respect to circuit diversity, central-office backup power, and diverse network monitoring.'' [9] To demonstrate that they are taking such reasonable measures, the rules require CSPs to annually certify that they have ''perform[ed] all the specific certification elements outlined in our rules regarding 911 circuit auditing, backup power at central offices that directly service PSAPs, and diverse network monitoring links.'' [10] CSPs may also meet these certification requirements by showing that they have implemented ''alternative measures . . . that are reasonably sufficient to mitigate the risk of failure, or that one or more certification elements are not applicable to its network.'' [11] In addition, CSPs must notify PSAPs of network outages that may affect the PSAPs' ability to receive 911 calls.[12] The Commission delegated authority to the Bureau ''to order appropriate remedial action on a case-by-case basis where 911 reliability certifications indicate such actions are necessary to protect public safety.'' [13]

Since the adoption of the 911 reliability rules in 2013, the Commission has revisited the rules on several occasions, but has not updated them to account for the transition to NG911. In 2014, the Commission issued a *Policy Statement and NPRM* on improving 911 governance and reliability, which reaffirmed the importance of 911 reliability and posited that changes in 911 technologies and a recent series of ''sunny day'' 911 outages indicated a potential need for further action.[14] Among the proposals advanced in the *NPRM,* the Commission sought comment on whether to broaden the definition of CSPs in former § 12.4 (now § 9.19).[15]

In 2015, the Commission issued a *Reconsideration Order* finding that the network reliability certification framework adopted in the 2013 *911 Reliability Order* was intended to allow flexibility for all CSPs to rely on reasonable alternative measures in lieu of any of the enumerated reliability practices set forth in former § 12.4(c) (now § 9.19(c)) of the rules, and that such flexibility was specifically intended to apply to the transition to NG911.[16] The Commission stated that ''flexibility is essential to support and encourage the transition to NG911'' and pointed out that, in the *911 Reliability Order,* the Commission stated that ''we intend today's rules to apply to current

[6] *911 Reliability Order,* 28 FCC Rcd at 17477, para. 2.

[7] *Id.* at 17477–78, paras 2–5; *Derecho Report* at 1–2.

[8] 47 CFR 9.19(a)(4)(i)(A)-(B). For ease of reference, we sometimes refer herein to PSAPs, statewide default answering points, and appropriate local emergency authorities collectively as ''PSAPs.'' The term ''covered 911 service provider'' does not include PSAPs or governmental authorities to the extent they provide 911 capabilities or entities that offer the capability to originate 911 calls where another service provider delivers those calls and associated number or location information to the appropriate PSAP. 47 CFR 9.19(a)(4)(ii)(A)–(B).

[9] 47 CFR 9.19(b).

[10] 47 CFR 9.19(c).

[11] 47 CFR 9.19(b); *see 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. 12 (2015), 80 FR 60548 (Oct. 7, 2015) (*2015 Reliability Recon. Order*). The designated corporate officer may fulfill the certification requirement by explaining how the communications service provider has undertaken alternative measures that mitigate the risk of 911 network failure. 47 CFR 9.19(c)(1)(ii)(A), 9.19(c)(2)(ii)(A), and 9.19(c)(3)(ii)(A). *See also 2015 Reliability Recon. Order,* 30 FCC Rcd at 8656–58, paras. 14–20 (confirming that, under § 12.4 (now § 9.19) of the Commission's rules, CSPs may implement and certify an alternative measure for *any* of the specific 911 certification elements, as long as the certification includes an explanation of how such alternative measures are reasonably sufficient to mitigate the risk of failure).

[12] *911 Reliability Order,* 28 FCC Rcd at 17526, para. 140; 47 CFR 4.9(h).

[13] *911 Reliability Order,* 28 FCC Rcd at 17534, para. 163. These rules improved upon the pre-existing requirement of telecommunications carriers, commercial mobile radio service providers, and interconnected voice over internet protocol providers to transmit all 911 calls to PSAPs. *See* 47 CFR 9.4, 9.10(b), 9.11(b).

[14] *911 Governance and Accountability, Improving 911 Reliability,* Policy Statement and Notice of Proposed Rulemaking, PS Dockets 14–193 and 13–75, 29 FCC Rcd 14208, 14222, para. 32 (2014), 80 FR 3191 (Jan. 22, 2015) (*2014 Reliability NPRM*).

[15] *Id.* at 14225, para. 42. The *2014 Reliability NPRM* also sought comment on ensuring transparency in connection with major changes in 911 service; ensuring reliability of IP-based 911 capabilities and services; and situational awareness and coordination of responsibility during outages. *Id.* at 14228, para. 48. Although the Commission did not act on the proposals from the *2014 Reliability NPRM,* we incorporate comments filed in response to the NPRM into today's item.

[16] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8654, para. 10. The Commission stated that the ''overarching purpose of the certification, including the attestation of a responsible corporate officer, is to 'hold service providers accountable for decisions affecting 911 reliability.' '' *Id.* (citing *911 Reliability Order,* 28 FCC Rcd at 17495–96 paras. 54, 59; 47 CFR 12.4(a)(3) (2015) (now 47 CFR 9.19(a)(3)). The Commission emphasized that ''[i]nflexible insistence on specified actions as part of each certification despite technical considerations that show those actions may not be appropriate in all cases would undermine this principle of flexibility without advancing the Commission's goal of improving 911 reliability.'' *Id.*

911 networks, as well as NG911 networks to the extent they provide functionally equivalent capabilities to PSAPs.'' [17]

In 2018, the Public Safety and Homeland Security Bureau (Bureau) issued a public notice seeking comment on the effectiveness of the 911 reliability rules, fulfilling a commitment made by the Commission in 2013 to reexamine the rules after five years to consider whether the rules were still ''technologically appropriate and both adequate and necessary.'' [18] In response to the *2018 Reliability Public Notice,* the Bureau received ten comments and six reply comments from entities representing industry, local government, and the public safety community.[19] The Commission did not take further action following the public notice, leaving the 2013 rules in place.

B. 911 Reliability Practices and CSRIC Recommendations

In 2018, the Bureau disseminated lessons learned from major network outages and reminded and encouraged communications service providers to review industry best practices to ensure network reliability.[20] The Bureau 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 in promoting industry best practices.[21] Based on the Bureau's analysis of several major network outages that affected subscribers, including those calling 911 for emergency assistance, the Bureau staff determined that providers could have likely prevented or mitigated the outages by employing certain network reliability best practices.[22] The Bureau encouraged communications service providers to implement certain industry best practices, as previously recommended by the Commission's Communications Security, Reliability and Interoperability Council (CSRIC),[23] including practices that could prevent or mitigate similar outages in the future.[24]

In 2019, in anticipation of additional entities transitioning to NG911, CSRIC VI issued a report and recommendations for 911 system reliability and resiliency.[25] The recommendations included measures to improve both legacy 911 and NG911, including ways in which the Commission could further the NG911 transition and enhance the reliability and effectiveness of NG911 through routing redundancy, maintenance, and mitigation of the threat of outages in both legacy 911 and NG911 systems.[26] The CSRIC recommendations address the need for service providers to (1) monitor for events resulting in loss of service; [27] (2) understand points of failure risks to (a) call delivery, (b) location delivery, and (c) callback information; [28] and (3) consider incorporating network detection tools and working with stakeholders to share information.[29] CSRIC VI also developed and recommended action for modifying or adding best practices regarding overall monitoring, reliability, notifications, and accountability in preventing 911 outages in transitional NG911 environments [30] as well as addressing cybersecurity considerations.[31]

In 2020, the Bureau updated the CSRIC Best Practices database.[32] The Bureau noted that CSRIC VII [33] unanimously approved an update to the database to include best practices from CSRIC VI (addressing communications network security, emergency preparedness, and disaster recovery) as well as the deletion of best practices that had become obsolete. The Bureau reminded and encouraged communications service providers to follow industry best practices to ensure network reliability, consistent with the CSRIC's recommendations, including ensuring (1) sufficient circuit diversity and alternative routing of 911 calls; (2) validating network changes in test environment, (3) using virtual interfaces and network management controls, and (4) making spare equipment available.[34]

C. 911 Interoperability

While the Commission has not to date adopted rules relating to 911 interoperability, in 2019, it directed CSRIC VII to survey the state of interoperability for the nation's 911 systems, including for legacy 911,

[17] *Id.; 911 Reliability Order,* 28 FCC Rcd at 17479, para. 9.

[18] *Public Safety and Homeland Security Bureau Seeks Comment on 911 Network Reliability Rules,* PS Docket No. 13–75, Public Notice, 33 FCC Rcd 5987, 5988 (2018) (*2018 Reliability Public Notice*); *911 Reliability Order,* 28 FCC Rcd at 17533, para. 159.

[19] The commenters to the *2018 Reliability Public Notice* were the Association of Public-Safety Communications Officials-International, Inc. (APCO); NENA: The 9–1–1 Association (NENA); West Safety Service; Alaska Communications; Texas 911 Alliance; Verizon; INdigital; USTelecom–The Broadband Association (USTelecom); Alliance for Telecommunications Industry Solutions (ATIS); Motorola; the Colorado Public Utilities Commission (Colorado PUC); AT&T; T-Mobile; CenturyLink; and the National Association of State 911 Administrators (NASNA).

[20] *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, 3776 (PSHSB 2018) (*2018 Best Practices PN*).

[21] *Id.*

[22] *Id.*

[23] For a general overview of CSRIC *see* FCC, *Communications Security, Reliability, and Interoperability Council, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0* (last visited Feb 14, 2025).

[24] *2018 Best Practices PN* at 3776–77.

[25] CSRIC VI Working Group 1, Final Report—Recommendations for 9–1–1 System Reliability 5 and Resiliency during the NG9–1–1 Transition 6 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*).

[26] *Id.* at 69.

[27] *Id.* (''There is a need for Service Providers across all industry segments (cable, wireline, wireless, Interconnected VoIP) to be able to identify within their networks service-impacting events that impair or cause a total loss of service.'').

[28] *Id.* at 70.

[29] *Id.* (recommending (1) ''Service Providers consider incorporating network detection tools, as appropriate, to assist network operations in detecting or deterring threats to 9–1–1 before they reach the ESInet perimeter'' and (2) ''Service Providers and other stakeholders work together to ensure that the system monitoring information that is needed to mitigate risks, monitor elements of the NG9–1–1 infrastructure and identify 9–1–1 outages is shared between providers and that the information is available to stakeholders when needed''). Working Group 1 also assessed the use of tools for Network Monitoring/Reporting to address the FCC's question: ''Are there tools commercially available that can detect or deter to mitigate an outage?'' The *CSRIC VI, WG 1 Report* included a matrix summarizing the responses and providing information ''on tools used to detect, deter and mitigate network anomalies within the 9–1–1 networks infrastructure.'' *Id.* at 70, Appendix A.

[30] *Id.* at Appendix B. In addition, CSRIC VI offers recommendations on how small and rural carriers can transition to NG911 while minimizing risks of the transition, such as preventative measures to avoid service outages. *See* CSRIC VI, Working Group 1, Transition Path to NG9–1–1, Final Report—Small Carrier NG9–1–1 Transition Considerations (2018), *https://www.fcc.gov/sites/default/files/csric6wg1sept18ng911report.docx.*

[31] *CSRIC VI, WG 1 Report* at 71 (recommending that (1) ''stakeholders take deliberate steps to consider the cybersecurity implications introduced by the transition to NG9–1–1'' and (2) ''a future CSRIC focus on NG9–1–1 related cybersecurity challenges and develop Best Practices as appropriate'').

[32] *See Public Safety And Homeland Security Bureau Announces Updates To The Communications Security, Reliability, And Interoperability Council Best Practices Database,* Public Notice, 35 FCC Rcd 577 (PSHSB 2020). The CSRIC Best Practices database can be accessed on the FCC website at *https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data* (last visited Feb. 14, 2025).

[33] FCC, *Communications Security, Reliability, and Interoperability Council VII, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii* (last visited Feb. 14, 2025).

[34] *See Public Safety and Homeland Security Bureau Encourages Communications Service Providers to Implement Important Network Reliability Practices,* Public Notice, PS Docket Nos. 11–60 and 20–183, 35 FCC Rcd 13179, 13179–80 (2020).

transitional 911, and NG911 networks.[35] In 2020, CSRIC VII Working Group 4 issued its report and recommendation on 911 interoperability, which were adopted by CSRIC VII. The report observed that 911 systems are highly interconnected, and interoperability between call-taking and call processing components is critical.[36] In addition, the report noted that ''[l]egacy, transitioning, and fully NG911-capable systems capture and exchange potentially large amounts of data and transferring such data between 9–1–1 systems potentially requires external data connections.'' [37] The report concluded that the state of national NG911 interoperability was 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.[38] The report 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.'' [39]

D. Next Generation 911 Transition Order

In July 2024, the Commission adopted the *NG911 Transition Order,* which established rules to create a consistent NG911 transition framework at the national level while also affording flexibility to 911 Authorities to modify the transition framework at the state, regional, local, territorial, or Tribal level.[40] The new transition rules specify a two-phased approach to guide the transition to NG911, in which 911 Authorities initiate each phase by submitting a valid request to OSPs within the relevant jurisdiction and OSPs must comply with NG911 requirements for that phase within a defined period. As part of the order, the Commission adopted a definition of ''Next Generation 911'' that includes interoperability, security, use of commonly accepted standards, and other criteria as core elements of the definition.[41] The Commission also noted the potential for NG911 to support improved reliability and interoperability and that some commenters had urged us to consider specific reliability and interoperability requirements.[42] While the Commission deferred consideration of these issues in the Order, it recognized that they warranted further scrutiny.[43]

The definition of Next Generation 911 adopted in the *NG911 Transition Order* also requires that emergency communications centers—*e.g.,* PSAPs—be able to receive, process, and analyze ''all types'' of 911 requests for emergency assistance.[44] The Commission explained that this language incorporates an accessibility component into the NG911 definition, and agreed with Communications Equality Advocates (CEA) that NG911 must support accessible technologies.[45] Several commenters urged the Commission to consider additional measures to enhance NG911 accessibility. While the Commission declined to address those proposals because they were outside the scope of that proceeding, it resolved to ''continue to monitor the development of NG911 systems and technologies'' and ''to take steps as necessary to ensure that NG911 is fully accessible to all.'' [46]

Discussion

A. The Need for Rules To Promote the Reliability and Interoperability of NG911 Networks

NG911 architecture offers distinct advantages over legacy 911 technologies, including the possibility of greater reliability, redundancy, interoperability, and accessibility.[47] In order to realize these advantages, however, NG911 networks must be designed to ensure resiliency and avoid potential single points of failure. Unlike legacy 911 networks, in which 911 call routing and delivery by a CSP typically occurs within the same service area as the destination PSAP, NG911 networks frequently aggregate traffic from various OSPs and widespread regions and transport it to geographically distant network components for processing and eventual delivery to ESInets for routing to the appropriate PSAP. In addition, NG911 network providers often contract with third parties to operate servers and other critical facilities that support 911 call routing and other key functions in multiple states and jurisdictions.[48] Without measures to ensure the resiliency of these critical components, failure of NG911 networks can lead to large, multistate outages. The introduction of NG911 and IP-based technologies therefore requires collaboration between industry, public safety participants including 911 Authorities, and the Commission to ensure that technology-enabled optimization does not introduce unacceptable risks that imperil 911 reliability, resiliency, and accessibility.[49]

Since the Commission adopted the 911 reliability rules for CSPs in 2013, the nation has continued to experience periodic ''sunny day'' outages that have impaired the ability of millions of Americans to access 911. While many of these outages have been local, some have been large, multistate outages associated with IP-based networks.

- In 2014, an outage in a service provider's 911 call-routing facility in Colorado caused 11 million people to lose 911 service for up to six hours, prevented emergency calls from reaching 81 PSAPs across seven states,

[35] CSRIC VII, Report on the Current State of Interoperability in the Nation's 911 Systems (2020) (*CSRIC VII WG 4 Report*), *https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.*

[36] *CSRIC VII WG 4 Report* at 5–6.

[37] *CSRIC VII WG 4 Report* at 5–6.

[38] CSRIC VII looked to the ''maturity states'' adopted by the FCC's earlier Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) to guide its report formulation. *See* TFOPA, Working Group 2, Phase II Supplemental Report: NG9–1–1 Readiness Scorecard at 13 (2016), *https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_Supplemental_Report-120216.pdf.* The TFOPA defined states of transition ranging 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 emergency communications centers (ECCs); are served by standards-based NG911 systems and/or elements; 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. *Id.*

[39] *CSRIC VII WG 4 Report* at 21–25.

[40] *NG911 Transition Order* at *2, para. 2.

[41] 47 CFR 9.28.

[42] *NG911 Transition Order* at **62–68, paras. 182–197.

[43] *Id.*

[44] 47 CFR 9.28.

[45] *NG911 Transition Order* at *17, para. 43.

[46] *Id.* at *61, para. 179.

[47] *Id.* at *62–64, paras. 182–183, 185–186; *id.* at *63, para. 185 (agreeing with 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 network withstood Hurricane Helene* (October 21, 2024), *https://statescoop.com/north-carolina-next-generation-911-hurricane-helene/* (quoting the Executive Director of North Carolina's state 911 board as crediting NG911 infrastructure for ensuring the continuity of 911 service through the Hurricane Helene disaster: ''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.'').

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

[49] *See, e.g., NG911 Transition Order* at **1, 12, 25, 60, 64, paras. 1, 29, 69, 176, 188.

and resulted in more than 6,600 calls to 911 never reaching a PSAP.

- In 2018, a service provider experienced a nationwide outage on its fiber network that lasted for one and a half days, affecting 22 million customers across 39 states, including approximately 17 million customers across 29 states who lacked reliable access to 911.
- In December 2022, an outage affected 911 calling for a service provider's VoIP customers in much of the South, and another service provider experienced two outages in 2022 disrupting 911 service to thousands in North Dakota and South Dakota for several hours.
- In February 2024, a provider experienced a nationwide wireless service outage that lasted at least twelve hours and rendered all voice and 5G data services unavailable for all users. More than 92 million voice calls were blocked, including more than 25,000 calls to PSAPs.
- In April 2024, a service provider experienced an outage caused by a cut fiber optic cable adjacent to its central office in Kansas City, Missouri. The outage disabled a portion of the provider's high-capacity transport network for 911 and non-911 traffic originated by various OSPs in different states, including 911 traffic that had first been collected by a 911 aggregator—a service provider that segregates and consolidates 911 calls from OSPs and routes them to the appropriate PSAP or ESInet.

Some of these recent 911 outages have exposed possible gaps in the coverage of the existing 911 reliability rules applicable to CSPs. The current rules relating to ''critical 911 circuits'' require CSPs to certify whether they have eliminated all single points of failure between the selective router, ALI/ANI databases, or equivalent NG911 components, and the central office serving each PSAP. However, in some of the multistate outages noted above, the vulnerabilities contributing to the outage were found to exist at points in the 911 call flow downstream from the OSP (which is already required under § 9.4, 9.10, or 9.11 to transmit all 911 calls to PSAPs) but upstream from either the selective router in legacy 911 environments or the ESInet in transitional or NG911 environments. In many cases, those points are operated by third parties that transport 911 traffic over high-capacity fiber from OSP networks to the ESInets that directly serve PSAPs. In other cases, OSPs segregate their 911 traffic and hand it off to 911 aggregation services, which deliver 911 traffic consolidated from multiple OSPs to PSAPs and ESInets. When these transport and aggregation components fail, they can interrupt 911 call flow to many PSAPs. Yet, because these components do not deliver calls directly to PSAPs at the local level, providers can argue that the components fall outside of the scope of the current reliability rules, particularly in the NG911 environment. We therefore believe Commission action is needed to address the reliability of these critical facilities in NG911 ecosystems. We seek comment on this analysis.

Another indicator of the need to revisit the 911 reliability rules for CSPs is that many of the multistate 911 outages reported to the Commission are ''sympathetic'' outages, *i.e.,* outages reported by one entity that are caused by a failure in the network of another entity.[50] Based on the data available in NORS, there have been at least 92 reported ''sympathetic,'' multistate outages in 2024 alone.[51] The Commission has noted that these ''sympathy reports contain information regarding service outages that, while caused by a failure in the network of another provider, nonetheless have an effect on the reporting service provider that may have public safety implications.'' [52] The high frequency and widespread scope of these sympathetic outages highlights the degree to which carriers increasingly rely upon large third-party service providers to aggregate and transport their traffic. These sympathetic outages usually are outside the scope of the existing 911 reliability rules, because CSPs can claim such outages occur in network elements that do not directly serve PSAPs and because the 911 reliability rules do not apply to OSPs. As a result, sympathetic outages expose a potential gap between our outage reporting and reliability certification rules, and the Commission currently has a limited ability to correlate reliability certifications with multistate outages reported in NORS.

When the Commission adopted the 911 reliability rules for CSPs, it committed itself to review the rules in the future ''to determine whether they are still technologically appropriate and both adequate and necessary to ensure reliability and resiliency of 911 networks.'' [53] The Commission stated that it would consider ''how NG911 networks may differ from legacy 911 service as well as outage reporting trends, adoption of NG911 capabilities on a nationwide basis, and whether the certification approach has yielded the necessary level of compliance.'' [54] Given the recurrence of major, multistate 911 outages, we believe the 2013 rules are not sufficient to safeguard 911 service in an NG911 environment, and that there are several ways that the current rules could be improved. We seek comment on this analysis.

First, the rules could more clearly specify which types of providers of NG911 capabilities qualify as CSPs that must comply with the reliability best practices in § 9.19 and file annual reliability certifications. The current rule refers to NG911 capabilities and/or ''functional equivalents'' of specified legacy capabilities. Although we believe that the Commission made clear its intent that NG911 capabilities be considered equivalent if they contribute to the routing of 911 traffic or to the storage or retrieval of associated location information, the generalized nature of this definition may explain why NG911 service providers are underrepresented among providers filing annual reliability certifications; of the 290 CSPs that filed 911 reliability certifications in 2024, only a small minority were NG911 providers. To the extent providers of NG911 capabilities are uncertain about whether they fall within the definition of CSPs, they also may not be implementing the Commission's reliability best practices.

The need for updating our rules regarding covered NG911 facilities is heightened by the fact that the entities operating the legacy 911 facilities that are highlighted in the rules—*i.e.,* selective routers and ALI/ANI databases—are retiring these facilities as they are superseded by NG911 networks.[55] As a consequence, continuing to rely solely on the 2013 rules to cover the transition from legacy 911 to NG911 could lead to reduced transparency and a weakening of reliability safeguards. Updating the rules to ensure that the functional equivalent standard clearly encompasses NG911 technology therefore should provide additional certainty that NG911 service providers are covered by our rules and improve the reliability practices of NG911 networks and the accessibility of NG911

[50] *See 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, 6160, para. 77 & n.156 (2021), 86 FR 22796 (Apr. 29, 2021) (*NORS Information Sharing Order*).

[51] This is based on reports identifying multiple states impacted by a reported outage, and does not include outages due to transport or SS7.

[52] *NORS Information Sharing Order,* 36 FCC Rcd at 6160, para. 78.

[53] *911 Reliability Order,* 28 FCC Rcd at 17533, para. 159.

[54] *Id.*

[55] *NG911 Transition Order* at *64, para. 186.

service. We seek comment on our view that updating the rules is needed to address these issues.

The reliability rules also do not address interoperability between ESInets—understandably so given that few ESInets existed when the rules were adopted in 2013. It has become clear, however, that one of the greatest potential benefits of NG911 technology is its ability to empower PSAPs to use ESInets to seamlessly transfer 911 calls and associated call data to other PSAPs that are better positioned to respond and deploy resources for emergencies. This life-saving benefit is an emerging one, but its potential will be substantially diminished if PSAPs cannot transfer calls to nearby PSAPs located across a state border, or if someone must retranslate or reformat the traffic to allow transfers to occur. In order to ensure that this capability exists nationwide, we believe we should consider adopting interoperability standards to facilitate the interstate flow of information between ESInets. We seek comment on our view that interoperability requirements are needed.

B. 911 Reliability

1. Expanding the Scope and Applicability of the 911 Reliability Rules

To account for the transition from legacy 911 to NG911, we propose to modify our definition of ''covered 911 service provider'' as follows. First, we would specify certain NG911 capabilities that satisfy the ''functional equivalent'' capability language of the current rule. Second, we propose to modify the current rule regarding what ''direct service'' to a PSAP or other answering point means, codifying language from prior Commission orders. Third, we propose to add five new NG911 CSP categories to cover both the expanding network gap between OSPs and state and local governments and the increasingly interstate and interlinked nature of NG911 ecosystem facilities. We seek comment on these proposals.

When the Commission adopted the reliability rules in 2013, it focused their application on service providers that, collectively, carry out the primary function of the 911 network: routing emergency calls to the geographically appropriate PSAP based on the caller's location.[56] The Commission recognized ''that overbroad rules could inadvertently impose obligations on entities that provide peripheral support for NG911 but may not play a central role in ensuring 911 reliability[.]'' [57] It therefore stated that it would only consider OSPs, internet service providers (ISPs), backhaul providers, aggregators, commercial data centers, and ESInets as CSPs to the extent they provide covered 911 capabilities directly to PSAPs.[58] The Commission further interpreted ''direct'' service to a PSAP to require a contractual arrangement or tariff agreement with the PSAP.[59]

The 911 facilities enumerated in the current definition of CSPs correspond to the rule's definition of ''critical 911 circuits,'' which comprise 911 facilities that originate at a selective router or its functional equivalent and terminate in the central office that serves the PSAP(s) to which the selective router or its functional equivalent delivers 911 calls, including all equipment in the serving central office necessary for the delivery of 911 calls to the PSAP(s).[60] Critical 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).[61]

When the Commission adopted the reliability rules in 2013, it declined to enumerate specific NG911 capabilities in the rules, because NG911 was still early in its development at that time, and the Commission expected that NG911 functionalities would evolve significantly in the future.[62] Instead, the Commission stated that it would consider NG911 service providers to be CSPs if they provided capabilities ''functional[ly] equivalent'' to the legacy routing capabilities enumerated in the rules or if they were the last service-provider facility connecting to a PSAP.[63]

The Bureau issued a Public Notice in 2018 that revisited the definition of ''covered 911 service providers.'' [64] Public safety and governmental commenters broadly agreed that the current definition of CSPs is too narrow, noting that it excludes the growing class of critical NG911 services that are provided by subcontractors and other parties that have no contractual relationship with PSAPs and therefore do not ''directly'' serve a PSAP under the current rules.[65] APCO, for example, asked the Commission ''to include any entity that provides 9–1–1, E9–1–1, or NG9–1–1 capabilities, directly *or indirectly*'' and reported that ''entities without a direct relationship to a PSAP have found methods to impact the ALI, routing, or supplemental data relevant to a 9–1–1 call.'' [66] The Colorado Public Utility Commission (COPUC) stated that the definition of CSPs ''should encompass any service or network component that could potentially impact 9–1–1 call delivery to the PSAPs, even if that service or network component is not directly contracted to deliver 9–1–1 calls and location information to the [PSAP].'' Comments from service providers mostly opposed broadening the definition of CSP. For example, the Alliance for Telecommunications Industry Solutions (ATIS) stated its belief that the current rules ''adequately encompass transitional and NG9–1–1 networks,'' and Motorola Solutions, Inc. (Motorola) requested that the definition be clarified by adding an express requirement that CSPs must have a direct contractual relationship with a PSAP.

The *NG911 Transition Order* requires OSPs to provide SIP-based 911 traffic to 911 Authorities (typically via ESInets) to enable those authorities to establish NG911 networks in their states. While establishing NG911 service brings inherent potential advantages to reliability and interoperability, the Commission did not seek to amend the 911 reliability or outage notification rules in that proceeding. Nevertheless, certain commenters suggested that the Commission update its rules to better address network reliability in an NG911 environment, including to encompass emerging classes of NG911 service providers.[67] We agree, and we

[56] *911 Reliability Order,* 28 FCC Rcd at 17478, para. 7 (citing the *Derecho Report* at 25).

[57] *Id.* at 17489, para. 37.

[58] 47 CFR 9.19(4)(i)(B); *911 Reliability Order,* 28 FCC Rcd at 17490, para. 39. Backhaul providers offer the infrastructure necessary to transmit data from one network point to another, often over long distances. For example, a mobile carrier may rely on a third-party backhaul provider to carry data from rural cell towers to its main network.

[59] *2015 911 Reliability Recon. Order,* 30 FCC Rcd at 8657, para. 17 (noting that CSPs are ''the entities with direct contractual relationships with PSAPs'').

[60] 47 CFR 9.19(5).

[61] *Id.*

[62] *911 Reliability Order,* 28 FCC Rcd at 17489, para. 36 & n.85.

[63] 47 CFR 9.19(4)(i).

[64] *2018 Reliability Public Notice,* 33 FCC Rcd at 5989.

[65] APCO Comments, PS Docket No. 13–75, at 1–2 (filed July 16, 2018); Daryl Branson, Colorado Public Utilities Commission Reply Comments, PS Docket No. 13–75, at 2 (filed Aug. 8, 2018); NENA Comments, PS Docket No. 13–75, at 1–2 (filed July 17, 2018); NASNA Reply Comments, PS Docket No. 13–75, at 2 (filed Aug. 13, 2018). *See also* 47 CFR 9.19(4)(i).

[66] APCO Comments, PS Docket No. 13–75, at 2 (filed July 16, 2018) (emphasis in original); *see also* NENA Comments, PS Docket No. 13–75, at 1–2 (filed July 17, 2018) (suggesting that the databases and software underpinning the infrastructure of the NG911 network should be included).

[67] *See, e.g.,* Windstream Reply Comments, PS Docket 21–479, at 2–3 (filed Sept. 8, 2023) (NG911

accordingly propose the measures described below.

Specification of Certain NG911 ''*Functional Equivalents.*'' We propose to amend the definition of ''covered 911 service provider'' to specify that NGCS Routing Facilities and NGCS Location Facilities are examples of NG911 capabilities that are functionally equivalent to the legacy facilities enumerated in the rule (*i.e.,* selective routers and ALI/ANI databases).[68] We further propose to define these NG911 capabilities consistently with the definitions adopted in the *NG911 Transition Order.* Together, these amendments would provide greater specificity for providers of these equivalent NG911 capabilities that they qualify as CSPs and are subject to the reliability standards in § 9.19 and the reporting requirements in § 4.9. We seek comment on this proposal.

We believe that these proposed amendments are consistent with the Commission's intent in adopting the current rule and would provide additional guidance as to the types of NG911 network functions and their associated network elements that are the ''functional equivalents'' of covered legacy routing facilities. The Commission explained in the *911 Reliability Order* that the routing of a legacy 911 call is accomplished via an aggregation point called a selective router, which identifies the PSAP that should receive the call based on the caller's phone number and address.[69] The selective router then determines the correct routing path for the call and transmits the call, 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 ALI and ANI databases before dispatching emergency services. Wireless 911 calls are routed similarly, but the caller's location must be determined using other technologies and third-party providers.[70] We set forth a simplified graphic representation of a legacy network below. Service providers operating the legacy facilities that perform essential routing and transmission capabilities—*i.e.,* selective routers and ALI and ANI databases—are clearly defined as CSPs in the current rule.[71]

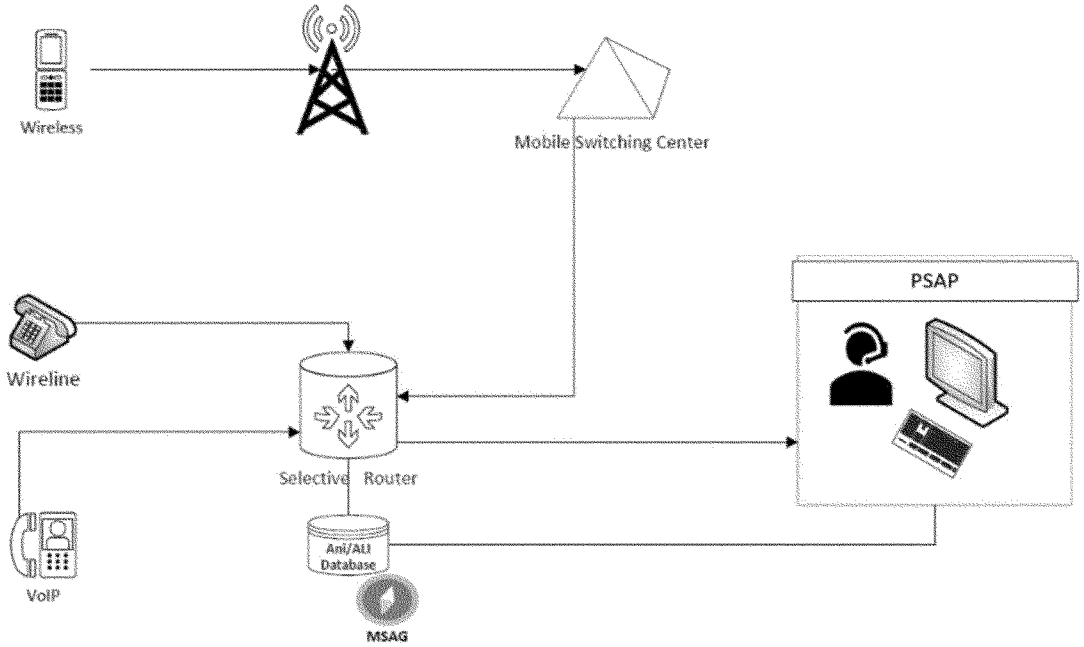

Figure 1- Legacy Network

traffic aggregators should be subject to the Commission's rules relating to disruption notification requirements, which currently apply to OSPs); Home Telephone Comments, PS Docket 21–479, at iii, 13 & n.6 (filed Aug. 9, 2023); *see also* NTCA Reply Comments, PS Docket 21–479, at 7–8 (filed Sept. 8, 2023).

[68] See proposed rules at §§ 9.19(a)(4)(i)(A), (B) and 9.19(a)(15)–(16).

[69] *911 Reliability Order,* 28 FCC Rcd at 17478–79, paras. 7–8 (describing the typical legacy 911 call flow); *NG911 Transition Order* at *4, para. 10.

[70] *911 Reliability Order,* 28 FCC Rcd at 17478–79, paras. 7–8.

[71] 47 CFR 9.19(4)(i). *See also NG911 Transition Order* at *4, para. 10 (legacy network diagram). The acronym MSAG refers to the Master Street Address Guide, which is replaced by the LVF in NG911 networks, while ANI/ALI databases are replaced by LISs. *NG911 Transition Order* at *31, para. 86.

In the *NG911 Transition Order,* the Commission recognized that ''[t]he transition to NG911 involves fundamental changes in the technology . . . use[d] to receive and process 911 traffic, and it requires equally fundamental changes in the way OSPs deliver 911 traffic to PSAPs.'' [72] The default NG911 rules adopted in the *NG911 Transition Order* require OSPs to deliver 911 traffic to an NG911 Delivery Point that each 911 Authority may designate within its state or territory.[73] From that demarcation hand-off point, 911 Authorities are responsible for transmitting 911 traffic to the PSAP(s), which may be accomplished through a combination of interconnected NGCS provided via the 911 Authority's ESInet(s).[74] These services may include Location Validation Functions (LVFs), Geographic Information Systems (GISs), Emergency Services Routing Proxies (ESRPs), Emergency Call Routing Functions (ECRFs), and Policy Routing Functions (PRFs).[75] The LVF is a server that validates civic location information against a GIS database to deliver more dynamic and actionable information about a caller's location than legacy ALI/ANI databases can.[76] GIS is a mapping system that collects, stores, and analyzes spatial data, ensuring that emergency services can pinpoint where to send help.[77] Next, an ESRP, which is a routing engine that determines the next hop for the 911 call, queries an ECRF, which is a database function that determines the appropriate destination PSAP by mapping the caller's validated location to maps with the boundaries of emergency response zones.[78] The call then is routed to the geographically appropriate PSAP in accordance with the PRF, which is a ruleset that decides how the call should be routed based on predetermined policies (*e.g.,* priority levels, time of day, and load balancing).[79] We set forth a simplified graphic representation of a Phase 2 NG911 network below.[80]

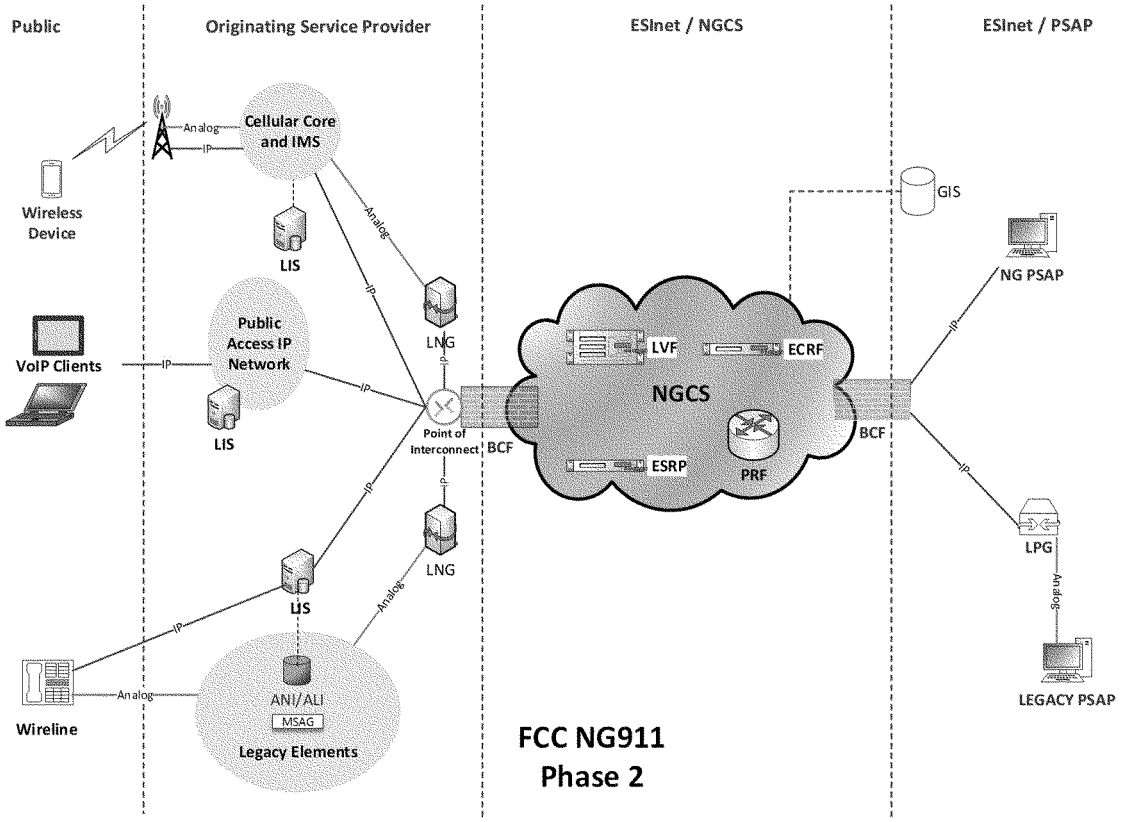

Figure 2 – Phase 2 911 Network

We believe the LVF and GIS core services are NG911 capabilities that are functionally equivalent to the ALI/ANI databases used in legacy networks. While they are not identical in a technical or engineering sense, we believe that these NGCS Location Facilities are equivalent in a functional sense because they similarly validate the 911 caller's location by reference to databases of geographical and civic data using information about the caller that

[72] *NG911 Transition Order* at *12, para. 28.

[73] *See id.* at *26, para. 71.

[74] *See id.* at *3, para. 6.

[75] *See id.* at **28–29, para. 79 (NG911 network diagram).

[76] *Id.* at **28, 31, paras. 78, 86; 47 CFR 9.28 (''An LVF is functional element in NG911 Core Services (NGCS) consisting of a server where civic location information is validated against the authoritative Geographic Information System (GIS) database information. A civic address is considered valid if it can be located within the database uniquely, is suitable to provide an accurate route for an emergency call, and is adequate and specific enough to direct responders to the right location.'').

[77] *NG911 Transition Order* at *65, para. 191; *see generally* NENA, NENA i3 Standard for Next Generation 9–1–1 at § 4 (Oct. 7, 2021), *https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-STA-010.3e-2021_i3_Stan.pdf* (*NENA i3 Standard*) (describing standard NGCS functions).

[78] *NG911 Transition Order* at *7, para. 17 & n.57; *NENA i3 Standard,* § 4.

[79] *NG911 Transition Order* at *65, para. 189, n.560; *NENA i3 Standard,* § 4.

[80] *NG911 Transition Order* at *28, para. 79 (NG911 network diagram). The acronym BCF in the diagram refers to the Border Control Function, which acts as a firewall between the ESInet and external networks.

has been provided by their OSP.[81] In turn, we believe that the ESRP, ECRF, and PRF core services are NG911 capabilities that are functionally equivalent to legacy selective routers, because they similarly determine the path along which to route 911 traffic so that it reaches the appropriate PSAP.[82] We refer to them collectively as NGCS Routing Facilities.

As has always been the case with § 9.19, this proposal, as well as those described below, are service provider agnostic. In other words, rather than designate certain entities as CSPs by virtue of regulatory status or industry category, we propose to continue to focus on the services provided and the facilities operated. We seek to preserve flexibility in a rapidly evolving technology market so that only entities that ultimately provide critical 911 functions in an NG911 environment are the ones subject to our rules. The goal is to ensure reliability, interoperability, and accessibility of critical NG911 facilities, not to predetermine market outcomes or to usurp or constrain state and local government decision-making.

We seek comment on these proposals and our analysis. Does the current definition of CSPs sufficiently encapsulate NG911 service providers, or should the definition specify which NG911 capabilities are the ''functional equivalent'' of the covered legacy routing and transmission services? Are LVFs, GISs, ESRPs, ECRFs, and PRFs examples of such functionally equivalent capabilities? Are these capabilities usually performed by non-governmental entities (*e.g.,* via contracts or agreements) or are there instances where they are performed directly by governmental entities? Are there other NG911 facilities or services that constitute functional equivalents? If so, what functions do they perform, and which legacy elements do they replace? Because CSPs may not uniformly fit the definition of ''telecommunications carriers,'' should we clarify that, similar to the requirement in § 9.4 of the Commission's rules, CSPs are required to transmit all 911 calls they receive to PSAPs? If not, on what basis should we treat CSPs differently from telecommunications carriers? We also request estimates of any new costs that would be caused by expanding the CSP definition in this manner.

As we propose to expand the classes of entities covered by our NG911 reliability rules to ensure that the rules capture entities that perform critical NG911 functions, we seek comment on whether we should conform § 4.5(e) in our outage reporting rules to similarly reflect this change. While § 4.5(e) already applies to NG911 outages, it does not specifically reference outages within the NG911 ecosystem facilities that we propose to define as critical (*e.g.,* Major Transport Providers, ESInet interconnection facilities, NGCS facilities, etc.).[83] Should these facilities be identified explicitly in the rule, and, if so, how? We also seek comment on whether we should amend the outage-reporting thresholds in § 4.5(e) to reflect additional outage impacts that are specific to the types of NG911 ecosystem facilities that we address in our proposed 911 reliability rules. If so, what should those NG911-specific outage effects be? The current rule includes a threshold of 900,000 user-minutes of lost communication with PSAPs. Are user-minutes (as defined in § 4.7(e)) the appropriate metric for outages that are specific to NG911 facilities? [84] If not, what metric would be appropriate?

Direct vs. Indirect Relationships with PSAPs. We propose to modify the requirement in the rules that providers of NG911 equivalent functionalities must ''directly'' serve a PSAP or other answering point in order to qualify as a CSP. The Commission included the ''direct service'' limitation in the original reliability rules to avoid imposing obligations on providers that ''may not play a central role in ensuring 911 reliability.'' [85] The Commission also recognized, however, that the scope of the CSP definition might need to ''be revised or expanded to cover . . . additional entities that provide NG911 capabilities, or in light of our understanding about how NG911 networks may differ from legacy 911 service.'' [86]

Modern NG911 networks have evolved to route 911 calls to PSAPs very differently from legacy architectures. In legacy networks, PSAPs typically contract with a single entity (such as an ILEC) to receive routing and location information services via a selective router and access to ALI and ANI databases, and they typically contract with the same entity to receive call delivery via trunk lines from the entity's nearest central office.[87] In contrast, NG911 routing is performed by many dispersed functional elements that may be operated by a variety of service providers, including OSPs, ESInet providers, their contractors, and other parties.[88] A PSAP or 911 Authority may not have contractual relationships with any or all of these entities.

We believe it is important that indirect providers of essential NG911 services comply with reliability best practices. As noted above, there was strong support for doing so among public safety and government commenters that responded to the *2018 Reliability Public Notice.* We are concerned, however, that including all indirect service providers within the definition of CSPs could unnecessarily increase the number of service providers that must file reliability certifications each year well beyond the increase we anticipate as a result of specifying certain NG911 capabilities that are ''functionally equivalent'' to covered legacy capabilities. That increase could drive up the operating costs of service providers—and, consequently, the costs for individual subscribers and 911 Authorities—and could interfere with the Commission's ability to closely review reliability certifications to identify and address problems.

We think the solution that best accomplishes our objective—while avoiding unnecessarily-burdensome certification and outage notification requirements—is to retain the direct service requirement but amend § 9.19 to state that CSPs directly serving PSAPs are responsible for ensuring the reliability of all of the NG911 capabilities they provide to the PSAP, whether through contractors of any tier, vendors, or via leased facilities. This proposal largely would be a codification of the longstanding principle that CSPs

[81] *See, e.g., NG911 Transition Order* at *64, para. 186 (''ALI/ANI databases will be replaced with IP-based systems with more precise location information[.]'').

[82] *See, e.g., id.* at *64, para. 186 (''Selective routers will be replaced with NGCS IP routing at the ESInet[.]'').

[83] We note that an outage that exhibits any of the effects of an outage described in § 4.5(e) would qualify as an ''outage that potentially affects a 911 special facility,'' regardless of whether the underlying 911 service is legacy 911 or NG911. *See* 47 CFR 4.5(e).

[84] ATIS argued in a prior proceeding that the outage threshold calculations set forth in §§ 4.5(e) and 4.7(e) are unsuitable for NG911 networks and that NG911 outage thresholds should be determined based on census or population data. *See* ATIS Comments, PS Docket Nos. 15–80, 13–75, at 15–16 (filed Jul. 30, 2021) (''Unlike legacy 911 systems, NG911 systems using the i3 architecture do not have access to telephone number counts. Legacy systems match a caller's phone number with information in the [MSAG] to determine a caller's location. With NG911 systems, calls are validated and routed using [GIS] data rather than the MSAG. Without telephone number counts, [CSPs] cannot calculate the number of user minutes potentially affected by an outage under Section 4.7(e) and thus cannot determine whether an outage potentially affects a 911 special facility under Section 4.5(e).'').

[85] *911 Reliability Order,* 28 FCC Rcd at 17489, para. 37.

[86] *Id.* at 17533, para. 159.

[87] *2014 Multistate 911 Outage Report* at 1–2, 14.

[88] *NG911 Transition Order* at *64, para. 186; *2014 Multistate 911 Outage Report* at 1–2.

must comply with § 9.19 reliability practices for facilities they lease from other parties, while the lessors themselves do not become subject to § 9.19 reporting requirements by making their facilities available to a CSP.[89] We believe this codification would ensure that reliability measures apply to essential NG911 functions while avoiding unnecessary burdens on providers and unnecessary distractions to PSAPs and 911 Authorities.

We seek comment on this proposal. Should providers of NG911 routing and transmission services be explicitly included in the definition of CSPs if they do not serve PSAPs directly? As the transition to NG911 has advanced, how typical is it for these types of services to be provided indirectly by entities with no contractual relationships with PSAPs? How are the relationships with these entities structured or memorialized? Would retaining the ''direct service'' requirement provide adequate oversight to the Commission and 911 Authorities? What advantages and disadvantages would this approach bring in contrast with simply requiring third-party, indirect providers to submit their own certifications? What would the cost impact be?

We also invite feedback on whether the proposed rules could hamper the flexibility of 911 Authorities to manage the implementation of NG911 in their jurisdictions. Would the rules interfere with 911 Authorities' procurement processes or unduly impact the cost of NG911 services? Would any of our proposals, if adopted, result in any existing contracts or agreements needing to be terminated or renegotiated, and, if yes, would that impact 911 service or costs or delay the transition to NG911? Would governmental entities prefer to have more or sole discretion over minimum reliability requirements or practices in their jurisdictions? How would eliminating the direct service limitation impact NG911 transition costs, and could it inadvertently slow NG911 deployments or discourage new market entrants?

We note that, during investigations of 911 outages, it is common for service providers to claim that they are contractually prohibited from sharing their contractors' confidential business information.[90] In response to one such claim, BRETSA argued that ''[i]f providers are contractually restricted from cooperating to provide information as to callers unable to reach 9–1–1 during an outage, then the Commission and the states must adopt rules permitting and requiring all providers to cooperate in supplying such information to PSAPs.'' How should the Commission address confidentiality concerns of indirect service providers? What is the appropriate balance for protecting and safeguarding non-public information (*e.g.,* proprietary business information) and creating and maintaining a reliable and resilient 911 system? Should 911 Authorities be allowed access to reliability certifications, and associated information, relating to indirect providers in addition to the certifications, and associated information, of CSPs?

Encompassing Other Essential NG911 Services. In order to improve the reliability of essential NG911 ecosystem facilities, we propose to add to the definition of ''covered 911 service provider'' the following classes of service providers that have emerged as critical to NG911 services: (1) operators of ''a Location Information Server (LIS) . . . or equivalent IP 911 location database;'' (2) operators of ''a Legacy Network Gateway (LNG) used for conversion of Time Division Multiplexing (TDM) 911 traffic to Session Initiation Protocol (SIP) . . .;'' (3) operators of Major Transport Facilities, which are ''[d]edicated SIP transport facilities meeting or exceeding Optical Carrier 3 (OC3) in capacity that collect and/or transmit IP 911 traffic, either segregated or mixed with non-911 traffic, originated from multiple OSPs and transported over interstate routes, for ultimate transport and delivery to an NG911 Delivery Point or ESInet''; (4) operators of IP Traffic Aggregation Facilities, which are ''[f]acilities that collect and segregate IP 911 traffic from non-911 traffic for multiple OSPs, or transport such traffic for ultimate delivery to an NG911 Delivery Point or ESInet;'' and (5) operators of ''interstate interconnecting facilities between ESInets.'' [91] We seek comment on this proposal, as discussed in further detail below.

a. Operators of LISs and LNGs

The framework adopted in the *NG911 Transition Order* addresses technology changes that are occurring in NG911 networks over the entire course of the 911 call flow, from origination to delivery to PSAPs. The in-state or in-territory NG911 Delivery Point serves as the demarcation point that presumptively divides responsibility for processing and transmitting NG911 traffic between OSPs on the one hand and 911 Authorities on the other.[92] The NGCS Location Facilities and NGCS Routing Facilities we discuss above address NG911 core services that are being provided on the 911 Authority side of the demarcation point.

On the OSP side of the demarcation point, the *NG911 Transition Order* requires OSPs that receive a valid request for NG911 service to incorporate certain NG911 functional elements into their networks, because those elements are necessary in order for ESInets to be able to route and deliver NG911 traffic

[89] *2015 911 Reliability Recon. Order,* 30 FCC Rcd at 8657, para. 17 (''[I]n cases where a party provides 911 services directly to a PSAP (pursuant to contract or tariff) over leased facilities, the auditing obligation would apply to that party, and not to the facilities lessor.' The Commission also suggested that [CSPs] could contract with facilities lessors, if necessary, to audit and tag leased circuits, but that the entity providing 911 service under a direct contractual relationship with each PSAP would remain responsible for certifying compliance with those requirements. We reaffirm those principles here, but clarify that [CSPs] (*i.e.,* the entities with direct contractual relationships with PSAPs) that rely on such contracts may implement and certify reasonable alternative measures as set forth above. We emphasize, however, that the contracting out of certain functions, or the determination of a PSAP to contract with more than one entity for various aspects of 911 service, does not absolve individual entities of their respective obligations for reliable 911 service.'') (citing *911 Reliability Order,* 28 FCC Rcd at 17506, para. 90); *see also, e.g., Eure Family Limited Partnership,* Memorandum Opinion and Order, 17 FCC Rcd 21861, 21863–64, para. 7 (2002) (''[T]he Commission has long held that licensees and other Commission regulatees are responsible for the acts and omissions of their employees and independent contractors.''); FCC, *Frequently Asked Questions: FCC 911 Reliability Certification, https://www.fcc.gov/frequently-asked-questions-fcc-911-reliability-certification#whocertify* (last visited Feb. 14, 2025) (''Where a Covered 911 Service Provider provides 911 services directly to a PSAP (pursuant to contract or tariff) over leased facilities, the circuit auditing obligation applies to the Covered 911 Service Provider, and not to the facilities lessor. Companies that directly serve PSAPs over leased facilities may contract with the lessor to audit those circuits or to provide some other assurance that they are physically diverse, but only the company with a direct relationship to the PSAP is responsible for certification.'').

[90] *See, e.g., 2014 Multistate 911 Outage Report* at 21–22 (''Intrado suggests that it is contractually precluded from providing the Commission or PSAPs with a clear understanding of what happened, adding that its business units are under contract to varying service providers and government agencies, and that 'those contracts are strictly honored.''' Intrado further asserted that ''it would be improper for [it] to 'cross the lines' established by its customers relative to information considered by them to be confidential in order for Intrado to 'glue together' a more complete picture of an outage for other parties, including, as the case may be, PSAPs or the Commission[.]'').

[91] See proposed rules at §§ 9.19(a)(4)(i)(C) through (G), 9.19(a)(12) and (13).

[92] *NG911 Transition Order* at *3, 26, paras. 6, 71. The *NG911 Transition Order* does not place any affirmative requirements on 911 Authorities. Instead, it invites 911 Authorities to adopt the Commission's NG911 framework, and, if they do, OSPs providing NG911 service to the 911 Authorities are assigned a series of performance and cost obligations from origination to the demarcation point in the absence of an alternate agreement with the 911 Authority. *See id.* at *2–3, paras. 2–7.

and to provide their full array of core services. First, the *NG911 Transition Order* requires OSPs to put into operation a LIS or its functional equivalent (or to acquire equivalent services from a third party) in order to verify their customers' location information.[93] That location information is then embedded with the 911 call and delivered to an NG911 Delivery Point or ESInet and is used by the ESInet's NGCS Location Facilities and NGCS Routing Facilities to route and deliver 911 calls. Second, in some cases, OSPs may be using an LNG (or acquiring equivalent services), in order to translate TDM-originated 911 traffic into SIP format before the 911 traffic is handed off to the ESInet.[94]

Because all 911 traffic must access LISs and all TDM-based 911 traffic must be converted to SIP format via LNGs, we believe it is critical that operators of these facilities employ reasonable reliability practices. The need for reliability is especially significant given that national carriers appear to be relying on a relatively small number of these facilities to service large portions of their networks and to deliver 911 traffic to ESInets across many states. We seek comment on our proposal to designate operators of LISs (or equivalent IP 911 location databases) and LNGs as CSPs.

b. Operators of Major Transport Facilities and IP Traffic Aggregation Facilities

When the Commission adopted the reliability rules in 2013, it excluded third-party transport providers and 911 aggregation services from the definition of CSPs because, at that time, they did not play a central role in the provision of 911 service.[95] We tentatively conclude that, in the decade that has since passed, these providers have become crucial to the provision of NG911 service at the interstate and national level, and, therefore, they should be subject to the same reliability and transparency requirements as other providers of covered services. We seek comment on this tentative conclusion.

Our understanding is that many OSPs now rely on high-capacity, IP-based fiber networks provided by third parties—which we refer to as Major Transport Facilities—to carry their 911 traffic to ESInets and PSAPs. These transport networks aggregate traffic (both 911 traffic and non-911 traffic) from multiple OSPs located in various states and carry it over long distances. The degree to which the 911 ecosystem has become dependent on these intermediate transport services is reflected in the outage investigations conducted by the Commission and by the outage reports submitted by OSPs through NORS. As we describe above, a number of multistate ''sunny day'' 911 outages have been caused by failures arising in or otherwise compromising Major Transport Facilities. Despite their outsized impact on 911 service, these networks currently fall within a gap in the Commission's rules; as providers of third-party transport service, they are neither CSPs nor OSPs, meaning they are not covered by the 911 reliability rules that are focused on routing and transmission services near the end of the 911 call flow nor by the Part 4 outage reporting rules relating to call originators and CSPs.

We wish to be cautious in how we define Major Transport Facilities so that § 9.19 continues to be focused on only the most critical 911 and NG911 elements and does not encompass smaller transport providers whose facilities do not pose a risk of widespread 911 outages. Accordingly, we propose to limit the definition Major Transport Facilities to providers that operate dedicated SIP transport facilities meeting or exceeding OC3 capacity; that also collect or transmit 911 traffic originated by multiple OSPs; and that also carry 911 traffic over interstate routes for ultimate delivery to an NG911 Delivery Point or ESInet.[96] We derive the proposed OC3 capacity from the outage reporting requirements in § 4.9. That rule requires ''outage reporting for communication disruptions impacting major transport facilities, specifically those with significant traffic-carrying capacity[.]'' [97]

Operators of IP Traffic Aggregation Facilities provide a niche service to OSPs: they segregate or collect segregated 911 traffic from OSPs and process and transmit the traffic towards the appropriate NG911 Delivery Points or ESInets.[98] We allowed the use of such services in the *NG911 Transition Order* because they ''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.'' [99] As with Major Transport Facilities, a large percentage of 911 traffic now passes through IP Traffic Aggregation Facilities. For example, one of these providers claims that it has ''deployments of NG911 call aggregation service in states and counties across the country'' [100] and that its 911 aggregation network serves 40% of the U.S. population. The provider claims to process more than 1.8 million 911 calls per month and to deliver the calls to more than 5,000 PSAPs.

We expect the roles of Major Transport Facilities and IP Traffic Aggregation Facilities to only increase as a result of the *NG911 Transition Order,* because it requires OSPs to deliver the 911 traffic they originate to NG911 Delivery Points that 911 Authorities may designate at any location within their state or territorial borders.[101] If these newly-designated traffic hand-off points are located outside of an OSPs' certificated service areas, OSPs may choose to procure the services of Major Transport Facilities and/or IP Traffic Aggregation Facilities rather than incur the high cost of building out their own networks.

We tentatively conclude that Major Transport Facilities and IP Traffic Aggregation Facilities have become critical to the overall reliability of the 911 ecosystem and that their operators therefore should comply with reasonable reliability standards. We

[93] *Id.* at *2, para. 3. *See also* 47 CFR 9.28 (formally defining a LIS as 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.''). ''A LIS [may] be a database, or [may] be a protocol interworking function to an access network-specific protocol. In NG9–1–1, the LIS supplies location (by value or reference) to the endpoint, or to a proxy operating on behalf of the endpoint.'' *NENA i3 Standard,* § 4.10 (emphasis removed).

[94] *NG911 Transition Order* at *26, para. 71.

[95] *911 Reliability Order,* 28 FCC Rcd at 17490, para. 39; *id.,* at n.90 (noting a commenter's argument that the reliability rules ''should apply to backhaul providers and aggregators of 911 call traffic'').

[96] See proposed rules at §§ 9.19(a)(4)(i)(E), 9.19(a)(12).

[97] *In the Matter of Amends. to Part 4 of the Commission's Rules Concerning Disruptions to Commc'ns; New Part 4 of the Commission's Rules Concerning Disruptions to Communications; The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband internet Service Providers,* PS Docket Nos. 15–80, 11–82, 31 FCC Rcd 5817, 5822, para. 11 (2016), 81 FR 45055 (July 12, 2016), 81 FR 45095 (July 12, 2016); *see also In the Matter of Amends. to Part 4 of the Commission's Rules Concerning Disruptions to Commc'ns; New Part 4 of the Commission's Rules Concerning Disruptions to Communications,* PS Docket No. 15–80, 30 FCC Rcd 3206, 3212–13, para. 19 (2015), 80 FR 34321 (June 16, 2015), 80 FR 34350 (June 16, 2015).

[98] See proposed rules at §§ 9.19(a)(4)(i)(F), 9.19(a)(13).

[99] *NG911 Transition Order* at *47, para. 138.

[100] Sinch, *NG911 call aggregator, Inteliquent, leads U.S. public safety, https://sinch.com/news/ng911-call-aggregator-inteliquent-leads-us-public-safety/?UTM-Inteliquent* (last visited Feb. 14, 2025). Sinch acquired Inteliquent in 2021.

[101] *NG911 Transition Order* at *55, para. 163.

seek comment on this tentative conclusion. Commenters in the *NG911 Transition* proceeding observed the important roles that these third-party entities have come to have.[102] We also believe that federal-level oversight of Major Transport Facilities and IP Traffic Aggregation Facilities is appropriate because they typically have multi-state or national footprints that exceed the scope of regulation or contractual terms imposed by any individual state or local government.

We seek comment on the inclusion of these providers in the definition of CSPs. Have Major Transport Facilities and IP Traffic Aggregation Facilities become critical to the reliable and interoperable transmission of 911 traffic to PSAPs? How frequently have outages impacting 911 originated within these facilities, and what were the causes and consequences of the outages? Would one or both of these definitions 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? Do our proposed definitions appropriately describe these providers, or should they be defined more narrowly or broadly? For example, should we update the ''OC3 and equivalent'' standard for Major Transport Facilities to ''1 Gbps (or 10 Gbps) Ethernet and equivalent,'' to better reflect modern IP transport facilities in use today? [103] Should we further limit the definition of Major Transport Facilities so that it refers only to facilities that carry a minimum volume of 911 traffic? If so, what is an appropriate minimum threshold? Should it be based on the number of 911 calls handled by the facility, on the number of OC3 minutes of 911 traffic, or some other metric? [104] Also, what specific costs would these providers incur if they were included as CSPs, and what would be the benefits to the reliability of the NG911 network? Are there other classes of providers that should be included as well, and why? [105]

c. Operators of ESInet Interconnection Facilities

Finally, we propose to designate interstate interconnecting facilities between ESInets as critical 911 facilities. As we explain in greater detail below, while ESInets are providing greater PSAP-to-PSAP interoperability within their areas of deployment compared to legacy networks, there is a concerning lack of interoperability between different ESInet providers. Interstate interoperability is especially low for the types of data associated with the advanced features that NG911 is meant to deliver, such as GIS-based location information, SMS text, and Multimedia Emergency Services (MMES), that enhance the accessibility of emergency services to persons with disabilities.

We do not propose requiring ESInets to adopt any particular technological solution to the interoperability problem, only that they take reasonable measures to provide reliable and interoperable 911 service and confirm their interoperability with other ESInets by conducting conformance testing. We expect, however, that whatever solutions ESInets adopt to become interoperable will require the exchange of potentially large amounts of data and may also require external data connections and therefore will be critical to the resiliency of NG911 service.[106] We therefore propose that these interconnection facilities should be treated as critical facilities that are subject to § 9.19 reliability standards and certification requirements. We seek comment on this proposal and on our analysis above. We also seek comment on how designating providers of interconnecting facilities between ESInets as CSPs would affect the accessibility of advanced, multimedia NG911 services for persons with disabilities, as well as estimates of cost impacts.

2. Reliability Requirements

a. Reasonableness Standard

We propose that any entity providing the foregoing critical NG911 capabilities or facilities be subject to the current requirement in § 9.19 to take ''reasonable measures'' to ensure reliability.[107] We believe moving to IP-based architecture in NG911 inherently improves reliability by enabling greater redundancy and geodiversity.[108] We further believe that it is reasonable for NG911 CSPs to ensure network reliability by adhering to prevailing industry standards.[109] We therefore tentatively conclude that these prevailing industry standards are achievable for CSPs at acceptable additional cost.[110] We further propose that CSPs may presumptively meet this

[102] *See, e.g.,* USTelecom Comments, PS Docket No. 21–479, at 5 (filed Aug. 9, 2023) (noting that NG911 systems will make it more challenging for wireline providers to comply with the Commission's 911 reliability rules, because 911 call traffic will be traveling over third-party networks); Windstream Reply Comments, PS Docket No. 21–479, at 2–3 (filed Sep. 8, 2023) (arguing that NG911 traffic aggregators should be subject to the Commission's rules relating to disruption notification requirements, which currently apply to OSPs); Home Telephone Comments, PS Docket No. 21–479, at 8, 14–17 (filed Aug. 9, 2023) (asserting that the use of NG911 call aggregators needs to be addressed to ensure reliability); NTCA Comments, PS Docket No. 21–479, at 4–5, 6–7 (filed Aug. 9, 2023) (predicting that NG911 will expand OSPs' use of third-party networks).

[103] *Is OC3 Bandwidth Still a Good Choice?,* GigaPackets, *https://www.gigapackets.com/articles/oc3bandwidth.php* (''The SONET family of line rates spans OC–1 at 52 Mbps on up to OC–768 at 40 Gbps. But in practice, only a few optical carrier levels are standard and readily available. These are OC–3 at 155 Mbps, OC–12 at 622 Mbps, OC–48 at 2.5 Gbps, OC–192 at 10 Gbps and OC–768 at 40 Gbps . . . Standard Ethernet WAN services mirror the standard Ethernet LAN speeds of 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps.'') (last visited Feb. 18, 2025).

[104] Note that we also are proposing to modify the 911 reliability certification form to ask NG911 CSPs to report the volume of 911 traffic handled by their facilities that do not conform to the Commission's reliability best practices.

[105] Bandwidth, Inc. argues that ''local exchange carriers' discontinuance of TDM services'' and a lack of ''alternative interconnection facilities, such as Ethernet'' is negatively impacting 911 reliability and the NG911 transition. *See* Bandwidth, Inc. *Ex Parte,* PS Docket 21–479, at 1–2 (filed Mar. 20, 2025). The broader TDM to IP technology transition is outside of the scope of today's *Further Notice.*

[106] *CSRIC VII WG 4 Report* at 5–6.

[107] 47 CFR 9.19(a)(4)(i)(A) and 9.19(a)(4)(i)(B) (applying rules to ''functional equivalent'' facilities and ''equivalent NG911 capabilities''); 47 CFR 9.19(b) (''All covered 911 service providers shall take reasonable measures to provide reliable 911 service with respect to circuit diversity, central-office backup power, and diverse network monitoring.'').

[108] *NG911 Transition Order* at *64, 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); *See also* Sophia Fox-Sowell, *North Carolina officials say next-generation 911 network withstood Hurricane Helene,* State Scoop (Oct. 21, 2024) (''‘Had the old technology and analog network still been in place, the infrastructure would have been destroyed . . . . Thanks to the resiliency and redundancy of this network, we had no reports of 911 calls not being delivered.'''), at *https://statescoop.com/north-carolina-next-generation-911-hurricane-helene/.*

[109] *CSRIC VI, WG 1 Report* at 115 (''Network Operators . . . should implement a continuous engineering process to identify and record single points of failure and any components that are critical to the continuity of the infrastructure . . . [and] pursue architectural solutions to mitigate the identified risks . . . .''), p. 124 (providers should ''design networks with redundant interconnectivity to'' ESInets), p. 122 (''Network Operators . . . should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering . . . functional redundancy and geographical diversity.'').

[110] *See e.g. Interstate Nat. Gas Ass'n of Am.* v. *Pipeline & Hazardous Materials Safety Admin.,* 2024 U.S. App. Lexis 20710, *22 (D.C. Cir. 2024) (''[T]he final rule invokes certain consensus industry standards that most operators already successfully utilize, so the incremental cost . . . would be negligible.'') (cleaned up); *see also Public Serv. Co.* v. *FCC,* 328 F.3d 675, 680 (D.C. Cir. 2003) (''In its analysis, the FCC approved of the Bureau's assessment of the prevailing industry standards'' to determine a reasonable pole attachment rate.).

reasonableness requirement by adopting reliability practices in three broad areas: physical diversity, network monitoring, and operational integrity (which as proposed will subsume and replace backup power).[111] We seek comment on these proposals.

Importantly, our proposed approach would retain the current structure of the 911 reliability regulations, which imposes a reliability ''reasonableness'' standard on all CSPs, subject to equitable remediation orders by the Bureau for failure to demonstrate reasonableness of network practices.[112] We propose to continue to allow CSPs to achieve presumptive reasonableness for specified CSP facilities by affirmatively implementing network practices described in the regulations.[113] This structure is designed to enable the Bureau to investigate [114] and validate network reliability based on filed certifications which show how well and how much of a CSP's network meets the Commission's standards. This process in turn enables the Commission to take preemptive actions to prevent outages before they occur. Bureau investigations can proceed by asking CSPs to provide information about the costs they would incur to upgrade their network reliability measures and assessing, from a cost-benefit standpoint, whether incurring such cost would be reasonable in light of the increased risk of critical 911 facility failure created by the CSPs' existing measures.

While we propose to keep the reasonableness standard that the Commission adopted in 2013, we propose to identify new ''best practice'' benchmarks for NG911 providers to allow them to presumptively satisfy the reasonableness requirement. We also propose to modify the process by which CSPs report alternative reliability measures to enable the Bureau to better assess reasonableness of network practices. We seek comment on this proposed framework, in tandem with the proposed reliability benchmarks below.

b. Benchmarks for CSP Demonstration of Presumptive Reasonableness

We propose to expand the range of required network reliability practices to ensure they better capture all relevant factors in the reliability of NG911 networks.[115] The Commission based its original 2013 rules ''on the *Derecho Report* and other prior experiences with natural disasters'' and therefore required reliability certifications only for circuit diversity, central-office backup power, and diverse network monitoring.[116] However, the Commission observed that as technologies evolve, ''categories based on legacy 911 networks may not adequately reflect reasonable measures to provide reliable service, particularly in an NG911 environment.'' [117]

We intend for today's proposed benchmarks for presumptive reasonability to capture the IP network engineering principles of reliability, resiliency, redundancy, physical diversity, and geographic diversity, which we believe most responsible NG911 network operators should be implementing. We wish to preserve the flexibility of PSAPs, 911 Authorities, and state governments regarding how best to allocate resources to meet their reliability needs,[118] while still adequately capturing the increasingly interstate and interlinked nature of NG911 where national standards may aid 911 Authorities.[119] Finally, our intent is that these NG911 reliability benchmarks would not apply to the origination of 911 traffic by OSPs, but would apply to service providers who aggregate 911 traffic or perform other critical NG911 functions and services for multiple OSPs.[120]

The purpose of these benchmark and certification proposals is to give the Commission reasonable oversight of CSP reliability practices while avoiding micromanagement of the network construction and design decisions of private entities. Accordingly, we do not propose to specify the details of reliable network practices down to the level of daily operational decisions and practices. Rather, we seek to articulate the kinds of measures that would demonstrate presumptive reliability when requesting certification. We seek comment on how best to improve 911 reliability and gather information that is reasonably actionable for efficient and

[111] 47 CFR 9.19(b) (''Performance of the elements of the certification set forth in [paragraph c] of this section shall be deemed to satisfy the requirements of this paragraph.'').

[112] *911 Reliability Order,* 28 FCC Rcd at 17492, para. 44 (''As discussed below, we adopt rules to require that Covered 911 Service Providers (1) take reasonable measures to ensure reliable 911 service and (2) certify annually that they do so by adhering either to specified, essential practices based on established industry consensus or to appropriate alternative measures demonstrated to be reasonably sufficient to mitigate the risk of failure.''). *See also* 47 CFR 0.392(j), 9.19(b).

[113] 47 CFR 9.19(b).

[114] 47 CFR 0392(h).

[115] *2014 Reliability NPRM,* 29 FCC Rcd at 14223–24, para. 37 (['']We seek to ensure that the Commission remains equipped, consistent with its statutory mandates and existing legal authority, with the proper regulatory tools to enforce continued and clear lines of accountability for reliable 911 call completion, including as the nation transitions to an IP-based NG911 architecture.''). The Commission noted, for example, the April 2014 multistate 911 outage resulted from a software coding error that disrupted routing of 911 calls and inadequate alarm management, which resulted in ''significant delays in determining the software fault and restoring 911 service to full functionality.'' *2014 Reliability NPRM,* 29 FCC Rcd at 14226, para. 43, *citing 2014 Multistate Outage Report* at 3.

[116] *2014 Reliability NPRM,* 29 FCC Rcd at 14226, para. 43 (internal quotations omitted).

[117] *Id.* at 14226, para. 43.

[118] *See, e.g.,* Texas 9–1–1 Entities Reply Comments, PS Docket No. 14–193, at 2, n.6 (filed April 21, 2015) (FCC reliability regulation of state contractors could increase the costs for PSAPs and state governments to hire contractors and delay NG911 transitions and deployments); NASNA Comments, PS Docket No. 14–193, at 2 (filed March 17, 2015) (PSAPs and 911 Authorities should be responsible for ensuring the reliability of 911 network services provided by their contractors); Washington Utilities and Transportation Commission Comments, PS Docket No. 14–193, at 3–4 (filed March 17, 2015) (911 oversight in Washington state is already shared by the Utilities and Transportation Commission, the Washington Military Department, and the E911 County Coordinators.'').

[119] Pennsylvania Public Utilities Commission Reply Comments, PS Docket No. 14–193, at 9 (filed April 21, 2015) (''The Pa PUC does support the development of a federal regulatory 'backstop' to eliminate gaps between federal and State authority. Where multi-state aspects of interlinked 911 network architectures exist, or where technology trends make vulnerabilities more likely or cause confusion to PSAPs and end-users, the Commission is best positioned to forge resolutions and develop national standards.''); Washington Utilities and Transportation Commission Comments, PS Docket No. 14–193, at 4 (filed March 17, 2015) (''Although it is true that technological and marketplace changes are altering the manner in which some components of 911 service are handled, including increasing reliance on network components and technology that are multi-state in nature, the vast majority of 911 calls originate and terminate within or to nearby PSAPs within each state and county and are jurisdictionally intrastate in nature. Accordingly, federal efforts should be dedicated to measures that assist, or complement, state and local governance efforts, rather than act to supersede them.'').

[120] *NG911 Transition Order* at *69, para. 202 (''. . . OSPs could significantly lower the overall costs of transmitting 911 calls to ESInets by taking advantage of third-party aggregators' services.''); *NG911 Transition Order* at *71, para. 206 (''CSRIC explains that LIS as a service is contemplated as an NG911 solution at 'minimal expense' to small OSPs, as it relieves OSPs of most costs beyond monthly services, and an LNG and can be provided either by a commercial vendor or the 911 authority.''); Home Telephone NG911 Notice Comments at iii (''[T]he Commission should focus on the back-end for-profit entities that aggregate front-end 911 transmissions from multiple jurisdictions, process, and then deliver via back-end connections IP-based information to the appropriate local [PSAPs]. 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.''); Bandwidth NG911 Notice Comments at 2–3 (''Bandwidth predominately acts as a VoIP Positioning Center ('VPC') where it provides stand-alone emergency location and 911 call routing capabilities for its VoIP service provider customers . . . . Bandwidth has a robust network that reaches across the United States and Canada and delivers around 3 million calls a year from 26.7 million end points . . . . To date, Bandwidth established network aggregation capabilities to route its customers' 911 traffic through 16 ESInets.'').

effective Commission and 911 Authority oversight, while also ensuring robust notice of ''reasonable'' reliability compliance expectations for CSPs. We also seek comment on whether adopting a reasonable reliability standard of ''five nines'' availability would be another valuable measure for determining compliance, or whether annual CSP facility availability time should be reported in addition to these benchmarks.[121] How should ''five nines'' availability be calculated? [122]

(i) Physical Diversity

We propose specifying that the critical IP paths subject to the rules be subject to physical diversity requirements appropriate to NG911 and transitional networks.[123] For legacy 911 circuits, the best practice benchmark of audits and tagging will remain the same. For NG911 facilities, we propose that ''physical diversity'' would mean that critical paths established by CSPs must be geographically diverse,[124] load-balanced,[125] and capable of automatic failover to the backup element (*e.g.,* redundant routers or node connections and links) and automatic reroutes to redundant paths in the transport layer in the event of path failure.[126] Redundant routers or node paths and links should be located in different geographic locations (*i.e.,* in different physical facilities). We seek comment on this proposal.

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. Importantly, we propose to add geographic diversity as a necessary part of this updated definition for IP paths, to ensure service providers can automatically re-route 911 traffic to travel over a different path that is both physically diverse *and* geographically separated. We seek comment on the appropriateness of geographical diversity as part of the physical diversity requirement for IP-based networks.

In 2013, the Commission included ''circuit auditing and tagging'' as an element of the 911 reliability rules, which requires CSPs to certify annually whether they have (1) audited the physical diversity of critical 911 circuits [127] or equivalent data paths to any PSAP served, (2) tagged such circuits to reduce the probability of inadvertent loss of diversity between audits,[128] and (3) eliminated all single points of failure in critical 911 circuits or equivalent data paths serving each PSAP.[129] If a CSP has not implemented the third element (*i.e.,* the elimination of all single points of failure), it must certify ''[w]hether it has taken alternative measures to mitigate the risk of critical 911 circuits that are not physically diverse or is taking steps to remediate any issues that it has identified with respect to 911 service to the PSAP.'' [130] Respondents also may certify that the circuit auditing requirement is not applicable because they do not operate any critical 911 circuits.[131]

In 2013, the Commission required CSPs to certify to circuit diversity measures for paths between a selective router or its functional equivalent and the central office serving a PSAP. The Commission further identified routing and 911 traffic aggregation as distinct functions performed by the selective router.[132] While this standard always applies to aggregated circuits when service is directly provided to a PSAP, under today's proposals if 911 traffic aggregation and routing are occurring at different points, both functions would trigger the requirement under our rules specify the examples that ''functional equivalence'' includes IP traffic paths from NGCS facility capabilities (when provided directly to PSAPs), or from an aggregation point located in a different central office from the selective router.[133] In 2014, the Commission introduced concepts such as dynamic routing, load balancing, automatic re-routing, and geographic facility diversity as reliability best practices for IP network paths and facilities.[134] In

[121] *See 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, p. 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* (''Mr. Rosen then explained that five nines is a term used in 911 systems to determine reliability of a 911 system, and the term refers to a 911 system being available 99.999% of the time. Mr. Rosen said there are two ways to determine availability. One way is to determine the actual availability of the system based on the period of time the system has been operational. In the alternative, availability can be determined by calculating two quantities: the mean time between failures and the mean time to repair for each component in the network.'') (*Nebraska PSC Order*).

[122] FCC, Task Force on Optimal PSAP Architecture (TFOPA), Adopted Final Report, p. 103, (2016), *https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf* (''While 'five nines' is the generally accepted minimum availability service level, it should be noted that this equates to 5.26 minutes of unscheduled downtime or service unavailability per year. Another important factor when comparing network availability to consider is specifically how different network service providers define availability and how it is calculated. For example, scheduled maintenance events are typically not included/classified as downtime. The ESInet by design incorporates multiple paths for voice and data transmission. The failure of a single element within the network or congestion along a path will not necessarily limit the ability to deliver traffic.'')

[123] *CSRIC VI, WG 1 Report* at 51 (''It is assumed in this Report that all network elements and transport facilities are deployed with redundancy'').

[124] *2014 Reliability NPRM,* 29 FCC Rcd at 14227, para. 45, n.106 (''For example, network architectures utilizing . . . databases in different geographic locations . . . will be more reliable and resilient than those that route all calls through a single active database . . . .'').

[125] *Id.* 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.'').

[126] *Id.* at 14227, para. 45.

[127] Critical 911 circuits are defined as ''911 facilities that originate at a selective router or its functional equivalent and terminate in the central office that serves the PSAP(s) to which the selective router or its functional equivalent delivers 911 calls, including all equipment in the serving central office necessary for the delivery of 911 calls to the PSAP(s).'' They also include automatic location information (ALI) and automatic number information (ANI) connecting circuits that originate at the ALI or ANI database and terminate in the central office that serves the PSAP. *See* 47 CFR 9.19(a)(5).

[128] The rules define tagging as ''[a]n inventory management process whereby critical 911 circuits are labeled in circuit inventory databases to make it less likely that circuit rearrangements will compromise diversity.'' Covered 911 Service Providers may use any system they wish to tag circuits so long as it tracks whether those circuits are physically diverse and identifies changes that would compromise such diversity. *See* 47 CFR 9.19(a)(11).

[129] *See* 47 CFR 9.19(c)(1)(i).

[130] 47 CFR 9.19(c)(1)(ii)(A).

[131] For example, small or rural local exchange carriers (LECs) may provide administrative lines to PSAPs but do not typically operate selective routers or control the facilities that connect selective routers to the central offices serving each PSAP. In such cases, they could respond that the circuit auditing element of the certification is not applicable.

[132] *911 Reliability Order,* 28 Rcd at 17478, para. 7 (''The local switch then sends the call to an *aggregation point* called a selective router . . .'') (italics added).

[133] See proposed rules at § 9.19(a)(4)(i)(A)–(B), § 919(a)5(i).

[134] *2014 Reliability NPRM,* 29 FCC Rcd at 14227, para. 45, nn.106, 107 (proposing to expand reliability certifications for NG911 to ensure IP-based 911 architecture is geographically distributed, load-balanced, and capable of automatic reroutes.'');

2015, the Commission observed that NG911 networks achieve reliability and resiliency with geographic diversity and dynamic routing instead of traditional TDM circuit auditing and tagging.[135] Today we propose to add critical paths of major transport facilities and 911 aggregation network facilities as subject to our physical diversity rules regardless of whether the provider has direct service contracts with a PSAP or other answering point.[136] Furthermore, we propose to codify additional physical diversity technical standards to encompass both legacy and NG911 facilities, to ensure that NG911 entities will no longer have to explain each year that they are using the IP ''alternative'' to legacy TDM 911 reliability. We seek comment on our assessment.

Finally, we seek comment on whether our proposed reliability measure for IP physical diversity is sufficiently inclusive, and on the likely compliance costs and lives-saved benefits from adopting this rule. We note that today's proposed rules are not meant to capture every single transit provider of general internet traffic, but rather dedicated transport providers that carry substantial 911 traffic.[137] Does the explicit inclusion of major transport paths and 911 aggregator networks capture enough of the critical 911 bottleneck infrastructure to reasonably improve 911 reliability? Or does this proposal sweep too many OSP operators of IP traffic-aggregated paths into the CSP category, and if so, what metric could be used to better distinguish the most critical 911 transport and aggregation points and paths which should be covered in an NG911 environment? Should we also designate additional paths to and from the LIS as covered critical paths, or would that expand the CSP category too far to include the majority of OSPs? In the alternative, should LIS and LNG operators be at least required to ensure physically diverse ingress and egress points *from* their facilities? What would the additional costs be of such an expansion of this benchmark?

(ii) Network Monitoring

In the 911 reliability rules adopted in 2013, the Commission required CSPs to certify whether they have taken the following steps to ensure reliable monitoring of critical components of their networks: (a) conducting audits of aggregation points for gathering network monitoring data, (b) conducting audits of monitoring links, and (c) implementing physically diverse aggregation points and links.[138] We propose to expand this existing requirement—which requires physical diversity between monitoring points and physically diverse links to network operations center (NOC) control points—by also including appropriate NG911 monitoring technologies identified in prior Commission orders as methods of compliance.[139]

We believe this revised rule should apply equally to both legacy and NG911 architectures. NG911-appropriate standards for network monitoring rely on automatic disruption detection and alarms.[140] The legacy 911 best practice of network monitoring via link and aggregation point audits[141] would continue to be a means of compliance for legacy facilities. In either case, network monitoring should ensure the performance of the critical NG911 ecosystem facilities of routers, LISs, and LNGs in real time by detecting failures, disruptions, or degradations in 911 service. We also propose that this new monitoring benchmark for IP networks should specify IP-appropriate monitoring of critical NG911 ecosystem facilities we identify today, including LNGs, LISs, and the IP routers responsible for path diversity. Should the IP monitoring benchmark be expanded further to interoperability capabilities, where applicable? We seek comment on our assessments and on this proposed benchmark.

(iii) Operational Integrity

The current ''backup power'' portion of the 911 reliability certification requires CSPs to indicate whether they provide at least 24 hours of backup power at any central office that directly serves a PSAP or at least 72 hours at any central office that hosts a selective router, and whether they have implemented certain design and testing procedures for backup power equipment.[142] We propose to retain this requirement for legacy central office facilities. However, we believe a modified requirement should be applied to NG911 networks to ensure continued operation in the event of a power outage.

IP-based NG911 facilities, especially when cloud-based, can reasonably be expected to have redundant and geographically distributed backups located in different facilities sufficient to ensure that a failure of any localized facility will not interrupt 911 traffic,[143] and should have appropriate continuous power, such as an uninterruptible power supply (UPS) device.[144] In 2014 the Commission observed that network architectures using ''two active databases in different geographic locations, each of which is capable of handling all 911 call traffic in the event of a fault in the other database, will be more reliable and resilient than those that route all calls through a single active database with backup equipment on passive ''standby'' mode.''[145] We seek comment on whether to codify this geographic diversity standard as a best practice benchmark to improve reliability. We also seek comment on whether requiring geographic diversity

Id., 29 FCC Rcd at 14243–44, Appx. A, Proposed Rules 12.4(a)(12) to (14), 12.4 (c)(4).

[135] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8656, para. 15.

[136] *See e.g. Nebraska PSC Order,* p. 40 (''While the Commission recognizes the failures were all between the aggregation point and the LNG, and not the ESInet nor core services, Lumen designed, installed and implemented this system and continues to be responsible for its failing infrastructure.''); *see also* CenturyLink Communications, LLC d/b/a Lumen Technologies Group's Responses to Commission Staff's First Set of Data Requests, at 4 (Dec. 1, 2023) (''Because of this outage, impacted calls never reached the NG911 network. The outage also impacted the SS7 links that connected to the [] aggregation point, preventing some OSPs' 911 calls from completing from that aggregation point.''), *https://psc.nebraska.gov/sites/psc.nebraska.gov/files/doc/Exhibit%20List%20%26%20Exhibit%201-30.pdf.*

[137] *NG911 Transition Order* at *47, para. 140 (commenters argue ''the Commission should establish rules requiring the transport of 911 traffic over dedicated SIP lines, and highlight that there are several options available to OSPs to comply with IP delivery rules with varying reliability . . . . We decline to establish the requested rules . . . . At this time, we provide flexibility to 911 Authorities, in concert with their NG911 vendors, to determine the IP-based SIP format to request from OSPs.''); *NG911 Transition Order* at *47, para. 140, n.414 (commenters ask the Commission to consider the costs of routing 911 traffic over a ''dedicated connection'' as opposed to ''best efforts public internet connections'') (internal citations omitted).

[138] *See* 47 CFR 9.19(c)(3)(i).

[139] *CSRIC VI, WG 1 Report* at 52 (''The NG9–1–1 SSP will be responsible for monitoring IP connections for transport alarms. Where appropriate, heartbeats may be used to verify the availability of network facilities. NG9–1–1SSPs should provide the means for capturing network traffic, generating alarms, and producing other metrics for monitoring and troubleshooting outages within NG Emergency Services Networks, as well as those impacting the ability of an NG Emergency Services Network to deliver calls to the target PSAP.'')

[140] *2014 Reliability NPRM,* 29 FCC Rcd at 14243, Appendix A, Proposed Rule 12.4(c)(3)(i)(D); *Id.,* 29 FCC Rcd at 14244–45, Appendix A, Proposed Rule 12.4(c)(5)(i)(A).

[141] 47 CFR 9.19(c)(3)(i)(1)–(2).

[142] *See* 47 CFR 9.19(c)(2)(i).

[143] *CSRIC VI, WG 1 Report* at 51 (''When the primary path is unavailable, the alternate path can be instantly deployed to ensure continuity of network services. As such the switching to a backup configuration, in general, does not cause service degradation.''); *see also 2014 Reliability NPRM,* 29 FCC Rcd at 14227, para. 45.

[144] *See e.g. FCC Urges Companies Using UPS Devices to Take Action Against Threats,* Public Notice (Apr. 7, 2022), *https://docs.fcc.gov/public/attachments/DOC-382138A1.pdf.*

[145] *2014 Reliability NPRM,* 29 FCC Rcd at 14227, para. 45, n.106.

at different physical facilities is robust enough to ensure reasonable reliability. Should we go further and require geographic diversity to mean redundant functionality housed in different cities or states, not just in different physical locations? Given the increasing size of natural disasters, what would be an appropriate distance requirement? Should we further expand the same IP operational integrity benchmark to monitoring interoperability facilities, diverse IP paths, and redundant routers, as well as to LIS and LNG facilities?

C. Interoperability

As noted above, the lack of interoperability is a known concern in NG911, which impairs and increases the cost of call and data transfer. CSRIC VII observed that the ''transition from legacy to IP-based networks, may result in hybrid system settings that commingle legacy and IP network elements. While in this hybrid state, the 911 systems operate at higher risk. For example, these systems may encounter challenges in ensuring interoperability with respect to 911 calls and related data.'' [146] CSRIC VII also observed that data collected by NASNA from showed low levels of interstate interoperability, particularly for data associated with NG911 such as location or SMS text as well as for features that enhance accessibility, (*e.g.,* Multimedia Emergency Services (MMES).[147] CSRIC VII found that ''[t]he more advanced technologies used day to day by the general public such as multi-media services had a very low level of respondents indicating interoperability.'' [148] As the NG911 transition progresses, these interoperability issues are likely to manifest into incompatibilities detrimental to the processing and receipt of 911 traffic and related information by 911 Authorities across state lines.[149]

To address these concerns, we propose to adopt interstate interoperability requirements to support the reliable exchange of interstate 911 traffic between ESInets. Specifically, we propose 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.[150] In that connection, CSPs would annually certify whether their interstate interconnecting ESInet facilities use conformance-tested equipment and whether they have tested their interstate interoperability capabilities. If a CSP cannot certify to these elements, we propose to require the CSP to certify with respect to those facilities: (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. We also propose to apply the definition of ''NG911'' adopted in the *NG911 Transition Order* to CSPs. Finally, we seek comment on the scope of our proposed interoperability requirements relative to other NG911 elements and whether to define interoperability to cover those elements.

1. Interstate Interoperability, Conformance and Interoperability Testing, and Interoperability Certification

Conformance and Interoperability Testing. We propose to adopt an interoperability best practice benchmark of testing and verification to support interstate interoperability. We recognize that there have been voluntary efforts to promote interoperability across NG911 vendors through best practices, standards development and conformance testing, but no national rules are in place for providers of NG911 capabilities. Conformance testing, a process generally planned and developed by industry organizations and conducted by certified labs, is a mechanism that could be used to ensure that devices and network equipment that are deployed are compliant with commonly accepted standards.

Consistent with our existing framework for reliability certifications, we propose that CSPs submit an annual certification of whether the equipment in their networks has undergone conformance testing and if not, whether they are using alternative measures to ensure interstate interoperability. Under our proposed approach, CSPs would be required to certify that they are able to process and share interstate 911 requests for emergency assistance and all associated information consistent with commonly accepted standards. We seek comment on this proposal. Is a certification approach sufficient to ensure that interoperability between ESInets across multiple states can be achieved without the need for proprietary interfaces, and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors? Should we require CSPs to certify that they are capable of maintaining interstate interoperability during a ''sunny day'' outage or disaster scenario?

We also seek comment on whether to adopt additional interoperability benchmarks, such as requirement to conduct interoperability testing between ESInets in addition to conformance testing of technology used by ESInets. Interoperability testing is an important mechanism for ensuring that CSPs are technically capable of supporting interoperability between states and different service providers. Unlike conformance testing, which can be used by a service provider to demonstrate its NG911 solution conforms to a standard and increases the likelihood of interoperability, interoperability testing involves two or more service providers to demonstrate the exchange of information. We therefore seek comment on adopting a benchmark that CSP perform interoperability testing with two or more ESInets in different states. To this end, we seek comment on requiring that CSPs annually test and certify that they have performed interoperability testing with at least two different providers in two different states, or if they are using alternative measures to satisfy interstate interoperability.

Interoperability Certification and Alternative Measures. We propose that CSPs submit an annual certification attesting to both conformance testing and interoperability testing starting one year after OMB approval of any associated information collection requirements. We seek comment on whether CSPs will be reasonably able to conduct the required testing within this time period. What processes or standards for test labs need to be in place before conformance testing can begin? Are there any other barriers to either conformance testing or interoperability testing that would impact being able to submit this certification?

Our proposed annual certification approach is consistent with our existing requirement under § 9.19(c).[151] We also propose to require CSPs to update their certifications annually to reflect any

[146] *CSRIC VII, WG 4 Report* at 5.

[147] *Id.* at Appendix B.

[148] *Id.* at 25.

[149] *See* Jackie Mines, *How is NG911 progressing?* (Feb. 11. 2025), *https://urgentcomm.com/911/how-is-ng911-progressing-* (''While the [NG911 i3] standards were written with interoperability in mind, if Vendor A interprets them differently than Vendor B, interfacing the systems doesn't go well and sometimes is nearly impossible.'').

[150] Under our proposal, ESInet interconnecting facilities operator refers to an entity that provides communication capabilities between ESInets.

[151] 47 CFR 9.19(c).

changes in their interoperability solutions that render prior certifications outdated. In addition, we seek comment on whether there are other methods, in addition to conformance testing and interoperability testing, for verifying that CSPs comply with ''commonly accepted standards'' and allow them to demonstrate that they are technically capable of providing interoperability. For example, is it necessary to specify end-to-end testing (typically required by the customer) and/or performance testing (testing that simulates a real world scenario)? [152] Are any such methods more reliable than conformance and interoperability testing for verifying interstate interoperability? What are the potential costs of, and challenges with, implementing any such methods?

Finally, we propose to adopt an alternative ''reasonable'' interoperability requirement for providers of interstate ESInet interconnecting facilities, following the same framework of § 9.19 for reliability. As with the current § 9.19 reliability certifications, CSPs would be allowed to either certify to meeting the interoperability benchmarks specified in the rules or to certify that they have achieved reasonable interoperability using alternative measures. We seek comment on this proposal. What alternative measures in lieu of our benchmarks would likely be used to certify and demonstrate ''reasonable'' interoperability? Should we require that CSPs successfully test the transfer of interstate calls between ESInets in order to demonstrate ''reasonable'' interoperability? What other alternative measures would demonstrate reasonable interoperability?

NG911 and Commonly Accepted Standards. We propose to amend § 9.19 of the rules to define providers of ''NG911'' capabilities by cross-referencing the definition of NG911 in § 9.28 of the rules. The definition adopted in the *NG911 Transition Order* helps define common sets of features and parameters at various points in the 911 call flow to allow any 911 call or text to be able to reach 911 call takers. We believe our proposal, consistent with the *NG911 Transition Order,* will help lay foundational elements to realizing interoperability between OSPs to 911 Authorities in multiple states. Under this proposal, CSPs would ''ensure interoperability'' and comply with ''commonly accepted standards'' similar to OSPs. Our proposed rule amendment would therefore ensure CSPs operate from the same baseline requirements to facilitate interstate interoperability and promote cooperation with OSPs. We seek comment on our proposal, including potential costs.

In addition, we seek comment on alternative approaches to ensure interstate interoperability. In response to the *NG911 NPRM,* some commenters urged us to clarify the roles of OSPs and providers of NG911 services.[153] APCO proposed that in addition to focusing on the delivery of 911 traffic by OSPs, the Commission should take the ''next step toward achieving public safety's vision for NG9–1–1'' by initiating a further notice of proposed rulemaking to address ''interoperability requirements for 9–1–1 service providers *and other elements of the emergency communications chain.*'' [154] In that connection, we seek comment from 911 Authorities and others as to whether we should expand the scope of our proposed interoperability requirement, and, if so, to what other elements of the emergency communications chain? Similarly, we seek comment on whether to amend § 9.19(a) of the rules to add a definition for ''interoperability'' for purposes of clarifying the obligations of NG911 service providers, including the definition of interoperability from the Spectrum Auction Reauthorization Act of 2023 (H.R. 3565), or some variation, for purposes of defining the scope of our interoperability requirements; and the potential benefits and costs of adopting such a definition.

Intrastate Interoperability. Today's proposals cover interstate interoperability between ESInets. With respect to intrastate interoperability, we believe that 911 Authorities can address NG911 interoperability within their jurisdictions pursuant to contracts and tariffs with providers of NG911 services and have the ability to order necessary testing and resolve interoperability disputes, including with sub-contractors, pursuant to such instruments. In addition, 911 Authorities are in the best position to address intrastate interoperability from the border control function at the in-state or in-territory NG911 Delivery Point through ingress to ESInet connected PSAPs and between PSAPs. We seek comment on our view.

2. Interstate Interoperability for Text and Video Accessibility

We seek comment on whether interoperability certifications relating to ESInet interconnection facilities should include specific certifications regarding interoperability of 911 text messaging and video accessibility consistent with the benchmarks discussed above. We believe that ensuring interoperability for non-voice NG911 communications is equal in importance to ensuring interoperability for voice NG911 calls. In the *NG911 Transition Order,* the Commission extended NG911 requirements to OSPs providing non-voice 911 services, including covered text providers and internet-based Telecommunications Relay Service (TRS) providers. NG911 is specifically intended to provide improved support for the full range of 911 voice, text, data, and video communications, including promoting and enabling 911 access for individuals with disabilities.[155] In its end state, NG911 will facilitate interoperability and system resilience, improve connections between 911 call centers, and support the transmission of text, photos, videos, and data to PSAPs

[152] *See, e.g., iCERT Interoperability Testing Report* at 10; Brian Rosen Comments, PS Docket 21–479, at 4 (filed Jul. 28, 2023) (''Call transfer across ESInets is now standardized in NENA STA–010.3, which is the standard that all current NGCS implementations are currently at or are expected to be upgraded to soon. Vendor testing at NENA ICE events and bilateral testing between vendors are proving interoperability today.'').

[153] *See, e.g.,* APCO Comments, PS Docket 21–479, at 4–5 (filed Aug. 9, 2023) (''The greatest impact the Commission can have on facilitating the transition to NG9–1–1 would be to require interoperability between OSPs and 9–1–1 service providers, and among 9–1–1 service providers.''); Jack Varnado, Livingston Parish Sheriff Comments, PS Docket 21–479, at 1 (filed Aug. 9, 2023) (urging the Commission to require all OSPs and 9–1–1 service providers achieve interoperability); Michael Coonfield, Oklahoma 911 Management Authority Comments, PS Docket 21–479, at 2 (filed Aug. 8, 2023) (stating that interoperability between ESInet and core services must be required and included in the forest guide); Texas 9–1–1 Entities Reply Comments, PS Docket 21–479, at 17 (filed Sept. 8, 2023) (''[T]he Commission should consider a notice of inquiry regarding interoperability between NG911 service providers, with emphasis on 911 call transfers between ESInets and within ESInets.'').

[154] APCO *Ex Parte,* PS Docket 21–479, at 2 (filed Apr. 18, 2024) (emphasis added). APCO previously urged the Commission to require interoperability between OSPs and NG911 service providers as part of the current proceeding. APCO Comments, PS Docket 21–479, at 2–4 (filed Aug. 9, 2023). However, in its *ex parte,* APCO expressed support for moving forward with the OSP requirements that the Commission proposed in the *NG911 Notice.* APCO *Ex Parte,* PS Docket 21–479, at 1 (filed Apr. 18, 2024). In a more recent *ex parte,* APCO urges the Commission to ''seek comment on a rule that would require 9–1–1 service providers to enable the ECCs they serve to exchange all forms of 9–1–1 traffic with ECCs in different states and/or served by different 9–1–1 service providers. Each 9–1–1 service provider could demonstrate compliance with this interoperability requirement by certifying that the ECCs it serves are able to exchange 9–1–1 traffic with at least three ECCs located in different states and/or served by other 9–1–1 service providers. Such a certification should include an attestation that the 9–1–1 service provider has confirmed interoperability through real-world testing at its sole cost.'' APCO *Ex Parte,* PS Docket 21–479, at 3 (filed Nov. 1, 2024).

[155] *NG911 Transition Order* at *74, para. 215.

by individuals seeking emergency assistance.[156]

We seek comment on how best to ensure that NG911 systems support interoperability for non-voice 911 services, with specific emphasis on text, video, and multimedia capabilities that support 911 access for people with disabilities. As noted above, NASNA's 2020 Interoperability Matrix reflected higher levels of interstate interoperability for 911 voice calls but no or low levels of interstate interoperability for all other services, including text-to-911 and MMES. We ask commenters to provide updated information on interstate 911 interoperability by type of service, with particular emphasis on services used by those with accessibility needs. For example, what are the current levels of interstate interoperability for the following types of service: (1) 911 voice calls; (2) location data; (3) text-to-911, including real-time text (RTT); and (4) MMES?

Text Messaging. Regarding text messaging, in response to the *NG911 NPRM,* Google and NENA proposed that we consider the implementation of new interoperable messaging protocols, such as Rich Communications Service (RCS).[157] We seek comment on Google's view that, ''[b]y addressing interoperable text messaging as part of its NG911 efforts, the Commission can further enable members of the public to connect to lifesaving resources, family members, and friends in a more effective and secure manner.'' Do commenters agree with NENA and Google's concerns about text interoperability and comments about RCS, and if so, would RCS fall under our definition of ''commonly accepted standards''? We seek comment more generally as to whether the public interest is better served by the Commission making such determinations in the short term or allowing the marketplace to make such determinations over a longer period of time. We also seek comment on whether there are interoperability problems in the commercial wireless market that are impeding end state end-to-end NG911? We invite commenters to comment on the specific connectivity, data transmission, and security issues Google describes as inherent in SMS/MMS. What options are currently available to address the aforementioned concerns as part of our certification requirements for CSPs, including intrastate interoperability requirements, and issues and what options do commenters foresee becoming available in the near-term and long-term?

Video. Point-to-point video calls can be instrumental to demonstrate the emergency at hand in order to expedite the provision of appropriate emergency assistance. Additionally, people with disabilities may benefit from video calling in order to communicate more clearly in conjunction with other modalities such as text communications. We seek comment concerning accessibility with particular focus on measures we can take to promote interstate interoperability between ESInets.[158] In response to the *NG911 NPRM,* commenter Brian Rosen suggested that the Commission could adopt requirements to ensure ESInets support three-way video for Video Relay Service (VRS) within a reasonable period of time, such as 12 months. Further, three-way video has the potential to support individuals with speech disabilities relying on speech-to-speech relay services.[159] Rosen claims that many vendors of NGCS systems plan to support video in upcoming releases and suggests imposing a regulatory deadline to do so. In addition, Communication Service for the Deaf, Inc. states that video sign-language communications in NG911 systems could occur in different ways, including through standard VRS, three-way video relay services,[160] or direct video calling (DVC). DVC would allow a caller who uses sign language to place a call to a call taker who is both fluent in sign language and trained in handling emergency calls, potentially eliminating the need for a third-party intermediary.[161] Should we amend our rules to require that NGCS systems support three-way video for relay services, and support DVC? If so, within what time frame should such support be required for either service? What conditions or qualifications, if any, should be included in requirements associated with these video calls? We seek updated data on interstate interoperability needed to meet the needs of the accessibility community, including the feasibility of providing DVC or three-way video 911 calls that include VRS, and challenges with implementation during the transition to NG911 and relevant timelines.[162]

We further seek comment on any potential efficiencies that three-way video and DVC, respectively, would achieve for PSAPs in NG911 systems. Could three-way video improve accuracy and efficiency for 911 call handlers to take an emergency call and dispatch the right assistance? Could DVC improve accuracy and efficiency in the handling of emergency calls? Could emergency calling-trained DVC call handlers located at regional or nationwide PSAPs send electronic dispatchable reports directly to the local PSAP, eliminating the need for intermediary interpretation? To what extent would three-way video and DVC services need to rely on each other's facilities and capabilities? [163] What role

[156] *NG911 Transition Order* at *6, para. 14; *NG911 Notice,* 38 FCC Rcd at 6209, para. 10.

[157] Google Comments, PS Docket 21–479, at 9–11 (filed Aug. 10, 2023); NENA Reply Comments, PS Docket 21–479, at 9–10 (filed Sept. 6, 2023). RTT is available in some locations as a text-based communications technology for 911 purposes. *See* FCC, *Real-Time Text, www.fcc.gov/rtt* (Nov. 5, 2024).

[158] *NG911 Transition Order* at *17, para. 43. In the *NG911 Transition Order,* the Commission adopted an NG911 definition that includes accessibility as an essential requirement, consistent with the definition in the Spectrum Auction Reauthorization Act of 2023 (H.R. 3565), which requires that NG911 ''be capable of processing 'all types' of requests.'' The Commission agreed that this requirement mandates that NG911 standards support accessible technologies. *NG911 Transition Order* at **14, 61, paras. 34, 179. The Commission declined, however, to expand the scope of the proceeding to consider accessibility issues raised in comments, but consistent with its authority under the CVAA, committed to monitor the development of NG911 systems and technologies and be prepared to take necessary steps to ensure that NG911 is fully accessible to all.

[159] *See, e.g.,* FCC, *Speech-to-Speech Relay Service (STS), www.fcc.gov/sts* (Jan. 28, 2025).

[160] Communication Service for the Deaf, Inc., *et al. Ex Parte,* PS Docket 21–479, at 2–3 (filed Mar. 12, 2025) (stating that traditional VRS uses a communications assistant fluent in sign language to enable a 911 caller to communicate through an intermediary, so that the VRS interpreter voices what the caller signs and signs back the call taker's response, while three-way video would allow the VRS caller, the 911 call taker, and the video interpreter to all be visible to each other on the same video call).

[161] *Id.* at 3. *See also Structure and Practices of the Video Relay Service Program,* CG Docket 10–51, Further Notice of Proposed Rulemaking, 32 FCC Rcd 2436, 2484, para. 125 (2017), 82 FR 17613 (Apr. 12, 2017), 82 FR 17754 (Apr. 13, 2017) (''A direct video calling (DVC) customer support service . . . permits individuals who are deaf, hard of hearing, deaf-blind, or have a speech disability . . . to engage in real-time video communication in ASL without using VRS. The purpose of DVC is to provide direct telephone service to such individuals that is functionally equivalent to voice communications service provided to hearing individuals who do not have speech disabilities.'').

[162] Brian Rosen Comments, PS Docket 21–479, at 5 (filed July 28, 2023) (stating that from the very first version (NENA 08–003), three-way video was a firm requirement and that the requirement was there expressly for VRS: a VRS user should be able to dial 9–1–1 and be placed in a 3-way video call with the caller, the 911 call taker, and a sign language interpreter).

[163] Communication Service for the Deaf, Inc., *et al. Ex Parte,* PS Docket 21–479, at 4 (filed Mar. 20, 2025) (''. . . ASL users use either a VRS app or a video communications device provided by their VRS provider to access 911 services. Each VRS company in turn contracts with an 'Emergency Call Relay Center' provider to facilitate the routing and processing of their 911 calls to the caller's appropriate PSAP . . . If the ability to use DVC is integrated into the NG911 infrastructure, could 911 calls placed by ASL-fluent callers be placed directly

should Emergency Call Relay Centers play in processing DVC calls? Would it be possible to route these calls to a call taker at an Emergency Call Relay Center (ECRC), who would then transmit the caller's information to a dispatcher at the appropriate PSAP? Should the Commission require all VRS providers to direct all incoming 911 calls to an ECRC upon receipt, to facilitate such direct communication? What are the costs and benefits associated with each of these services? What modifications to the NG911 architecture would be needed to enable DVC calls? What modifications would be needed to enable three-way video?

We also seek comment regarding current IP-based relay [164] provider capabilities and how to expand them. Do commenters agree that IP-based relay services providers currently supply a VoIP audio connection through a VPC, and that, to support video 911 calls, these providers would have to provide a video and audio connection, which current VPCs cannot handle? To enable IP-based relay services providers to support such calls, should we amend our rules to require ESInets to support internet connections, including video, via VPNs, to the ESInets, and if so, within what time frame, and subject to what conditions or qualifications? In that connection, do commenters agree with Brian Rosen that, to support three-way 911 video calls, IP-based relay providers would need to use the NGCS bridge, because bridges are used extensively in NG911 system to support attended transfer (so the call taker(s) can hear/see the call while they are completing the transfer—911 calls are not placed on hold)? If so, would this represent a change to their current process, which uses a Provider bridge, at least when supporting Voice carryover/hearing carryover? What are the costs associated with requiring three-way video support at the ESInet, and would such a requirement ensure equivalence for callers who are deaf or hard of hearing or have a speech disability?

D. Implementation and Oversight

In order to assist in monitoring compliance with our proposed rules for NG911 reliability and interoperability, we propose to update our 911 reliability data collections and oversight mechanisms. In the *911 Reliability Order,* the Commission stated that ''if a Covered 911 Service Provider certifies that it has taken alternative measures to mitigate the risk of failure, or that a certification element is not applicable to its network, its certification is subject to a more detailed Bureau review.'' [165] If the Bureau's review indicates that a provider's alternative measures are not reasonably sufficient to ensure reliable 911 service, the Commission stated that the Bureau should first engage with the provider and other interested stakeholders (*e.g.,* affected PSAPs) to address any shortcomings. To the extent that such a collaborative process does not yield satisfactory results, the Commission stated that the Bureau may order remedial action consistent with its delegated authority.[166] The Commission intended this process to allow flexibility to employ alternative—but reliable—network designs and technologies, not to create an exception that would swallow the rule.[167]

As discussed below, we believe that revised reporting requirements would be helpful to Commission staff and 911 Authorities in identifying risks to the reliability and interoperability of 911 traffic, including single points of failure, and ask commenters to identify specific information that providers should include in their certifications. We also seek comment on measures the Commission could take to limit the burden of reporting on NG911 reliability and interoperability. We also seek comment on how to better identify single points of failure that could have cascading effects on 911 traffic in multiple states. To what extent could the Commission limit the burden of any reporting requirements by providing increased flexibility for providers or businesses identified as small by the Small Business Administration? [168] We also propose to require disclosure of reliability and interoperability certifications to 911 Authorities. In that connection, we seek comment on establishing procedures for 911 Authorities to report concerns to the Bureau to conserve limited resources and focus attention on critical elements that could result in multistate outages or hamper interstate interoperability. We tentatively conclude that improving 911 Authorities' access to information about the 911 reliability measures in place within their states would amplify the Commission's ability to address potential risks to NG911 service and enable 911 Authorities to assess taking their own measures to prevent and mitigate disruptions to 911 service in their jurisdictions. We seek comment on this tentative conclusion and on the specific proposals below. In addition to enhancing reporting requirements for providers and improving information sharing with 911 Authorities, we seek comment on whether we should establish a dedicated consumer portal for 911-related outage complaints. Such a portal could provide the public with a clear and accessible means to report concerns about 911 service disruptions directly to the FCC. This approach may improve the Commission's ability to identify and address potential risks to NG911 reliability while empowering consumers to play a more active role in ensuring public safety. We invite input on the potential benefits of this proposal, including how it could complement existing reporting mechanisms and enhance transparency in addressing 911 service reliability.

1. Reform of Reliability Certification Process

Traditionally, NG911 CSPs select ''alternative measures'' to report reliability practices that differ from the legacy 911-specific best practice benchmarks articulated in our existing regulations, but which the Commission deemed reliable in the *2015 Reliability Recon. Order.*[169] We seek comment on whether one potential improvement from today's proposed changes of both defining NG911 equivalents and functional equivalents and codifying the best practice measures applicable to IP-based networks would be allowing NG911 CSPs to directly certify that they meet the benchmarks specified in our regulations, instead of having to use the alternative measures option to report IP-based network reliability practices. We seek comment on the impact of this change, and on related proposed minor changes described below.

In 2015, the Commission observed that NG911 networks achieve reliability and resiliency with geographic diversity and dynamic routing instead of traditional TDM circuit auditing and tagging, so the existing 911 reliability certification rules did not apply well to

to an ASL-fluent 911 call taker without being routed through a VRS provider?'').

[164] This would include VRS, IP Relay Services, and certain forms of IP Captioned Telephone Services.

[165] *See* 47 CFR 0.392(j); *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).'').

[166] *See 911 Reliability Order,* 28 FCC Rcd at 17497 para. 63.

[167] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8654–55, paras. 2, 10–11.

[168] For example, the Commission's requirements for live call data reporting provide a reduced reporting schedule for non-nationwide CMRS providers. 47 CFR 9.10(i)(3)(ii)(D).

[169] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8656–57, paras. 12, 15.

NG911 networks.[170] The Commission similarly observed that the existing monitoring benchmark was appropriate for legacy 911 facilities but not IP facilities, as IP-based service providers do not ''audit'' monitoring circuits the way TDM providers do, but rather use the automated network monitoring capabilities for their resilient IP-enabled networks.'' [171] At the time, the Commission did not undertake revision of the certification form, but rather instructed NG911 CSPs to report that they are using ''alternative measures'' for reliable IP best practices, since the CSPs could not realistically certify to using TDM-specific best practices on IP networks.[172] Accordingly, NG911 providers currently answer the legacy 911 certification questions in the negative, but then provide narrative descriptions of how IP network reliability differs from legacy 911 reliability.[173]

We seek comment on whether specifying NG911 and IP-based network benchmarks directly in the rules will allow NG911 CSPs to more easily certify to meeting reasonable reliability best practices without having to describe alternative measures for the compliant IP-based network facilities they operate, reserving alternative measures for deviations from the best practice benchmarks. If so, will this proposed change improve Commission collection and analysis of certification reliability data? What are the pros and cons of this approach in terms of data reported and collected? What drawbacks are there to this approach? Should the certification form be revised to require drop-down selections for the kind of legacy or NG911 facilities being certified to (*e.g.,* selective router central office, path from selective router to central office serving PSAP, major transport path to ESInet, LIS facility, etc.) to ensure clarity of which best practice standard (legacy or NG911) is being certified to? [174] We propose to direct PSHSB to consider revisions the certification form so that CSPs can specify which type(s) of 911 facilities they are operating—legacy and/or NG911—in a way that constrains which best practice standard they are certifying to. We further direct PSHSB to consider revisions to the certification form in ways that will ensure NG911 CSPs do not have to submit narrative explanations of alternative measures for IP-based facilities if those facilities meet the regulatory best practice benchmarks for IP-based networks. Will this change help the Commission identify which filers are proving NG911 services, which are providing legacy 911 services, and which are providing both? Would these changes also reduce the number of times CSPs have to answer portions of the certification form with ''not applicable,'' if the kind of facilities they operate and select from the drop-down menu automatically constrain which reliability and interoperability benchmarks they may certify to? We seek comment on these assessment and proposals.

Accordingly, we propose to direct PSHSB to revise the reliability and interoperability certification form to replace the current free-form text reporting option for alternative measures or ''not applicable'' answers with specified drop-down selection answers as determined by the Bureau, and to seek comment on a revised certification form. We tentatively conclude that this approach will best illuminate network practices for Commission staff and potentially reduce burdens on CSP filers. Similarly, if the updated form asks CSPs to select alternative measures and then list all facilities that employ them instead of vice-versa as it is now, we believe this will also improve reporting. We seek comment on this proposal.

We further propose modifying the certification form to ask NG911 CSPs to report on the volume of 911 call traffic that their non-conforming facilities handle. In response to a previous request for comment,[175] state government parties suggested improvements to the certification system to enable the Commission to determine the size of potentially impacted populations from critical 911 facility failures.[176] We believe most CSPs handling NG911 traffic from multiple OSPs have this data readily available,[177] and so such reporting would constitute a minimal burden to providers while providing valuable data to the Commission and to 911 Authorities.[178] We therefore believe such a change would improve 911 reliability and oversight with minimal additional burden on regulated entities. We seek comment on this proposal, on the best metric and reporting format to use for 911 traffic volume data, and on any additional suggestions for improving the certification form. Should the proposal be expanded to require 911

[170] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8656, para. 15 (''The circuit auditing requirement adopted in the 911 Reliability Order was based upon a CSRIC best practice urging network operators to 'periodically audit the physical and logical diversity . . . of their network segment(s) . . . .' [H]owever, appropriate measures to preserve physical and logical diversity may differ between circuit-switched time division multiplexing (TDM) and IP-based networks because IP-based routing and . . . re-routing can occur dynamically over many possible paths.'').

[171] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8659, para. 20.

[172] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8656, para. 12 (''[W]e clarify that the certification framework adopted in the 911 Reliability Order allows flexibility for all Covered 911 Service Providers—legacy and IP-based—to certify reasonable alternative measures to mitigate the risk of failure in lieu of specified certification elements.''); *2015 Reliability Recon. Order,* 30 FCC Rcd at 8657, para. 16 (''Technology transitions have already resulted in a variety of hybrid 911 network architectures in which some functions are provided over legacy TDM circuits and others are provided over IP-based infrastructure. In such cases, our rules as revised will permit the provider to certify reasonable alternative measures with respect to either portion of the network.'').

[173] *2015 Reliability Recon. Order,* 30 FCC Rcd at 8657, para. 16 (''[E]xplanations of alternative measures with respect to circuit audits and tagging should . . . describe affirmative steps in lieu of audits and tagging to mitigate the risk of a service disruption. . . .'').

[174] *See 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).

[175] *See 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, 4414–5 (PSHSB 2020).

[176] 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.''); Colorado Public Utility Commission Comments, PS Docket 13–75, at 2 (filed July 8, 2020) (same).

[177] *See e.g.,* Bandwidth Comments, PS Docket 21–479, at 2–3 (filed Aug. 9, 2023) (''Bandwidth predominately acts as a VoIP Positioning Center ('VPC') where it provides stand-alone emergency location and 911 call routing capabilities for its VoIP service provider customers. . . . Bandwidth has a robust network that reaches across the United States and Canada and delivers around 3 million calls a year from 26.7 million end points. . . . To date, Bandwidth established network aggregation capabilities to route its customers' 911 traffic through 16 ESInets.''); Inteliquent Reply Comments, PS Docket 21–479, at 1 (filed Sept. 8, 2023) (''Sinch provides a Voice over Internet Protocol ('VoIP') Positioning Center ('VPC') service to VoIP providers. Sinch's VoIP customers contract with Sinch to facilitate VoIP 911 call delivery to the appropriate Public Safety Answering Points ('PSAP').'')

[178] Inteliquent *Ex Parte,* PS Docket 21–479, at 1 (filed Oct. 10, 2023) (''. . . Sinch explained that a subset of Next Generation Core Services Providers ('NGCS Providers') rely on Sinch to assist with steering Automatic Location Information (''ALI'') queries between PSAPs and Sinch's Voice over Internet Protocol Positioning Center ('VPC') platform via the ALI Database or Location Database ('ALI/LDB'). These NGCS Providers are considered Covered 911 Service Providers under the FCC's rules.'').

traffic volume reporting for conforming facilities as well?

We further propose to direct the Bureau to consider additional ways to improve the certification forms pursuant to its delegated authority.[179] The 911 reliability and interoperability certification submission form and data should simultaneously: (1) ensure the Bureau can reasonably perform its investigation [180] and Remediation Order [181] delegated responsibilities to facilitate 911 reliability and interoperability; (2) provide similar reasonable oversight for 911 Authorities; and (3) impose no greater reporting burdens on CSPs than is necessary for these purposes. We direct the Bureau to prepare to appropriately implement such improvements bearing these factors in mind, consistent with today's rule proposals.

In connection with the above, we propose minor amendments to consolidate rule 9.19 in some instances, to minimize the burden on regulated entities subject to these rules by making it easier for them to identify and comply with all 911 reliability and interoperability requirements. For example, propose to consolidate the alternative measures reporting paragraphs at § 9.19(c)(1) to (3) to similarly capture both legacy and NG911 providers, and to better ensure the Bureau can revise the annual certification form to best respond to 911 Authorities' needs and obtain necessary data to make a reasonableness determination under its delegated authority.[182] We also propose to consolidate and streamline the record retention paragraphs under § 9.19(d)(3) to better apply across all legacy and NG911 CSPs. We seek comment on these modifications, and any other advisable non-substantive or conforming edits to rule 9.19.

Finally, we seek comment on whether there are measures in addition to annual certification that would promote 911 reliability and interoperability. For example, could the Commission implement an outcome-based standard that establishes how many annual user minutes of 911 traffic could be interrupted by network or facility outages and still be considered reasonable, beneath which a CSP is subject to remediation orders? Could the Commission adopt a similar interoperability standard based on percentage of interstate 911 call transfers which fail completely, or fail to include caller location or other data?

2. Access to Reliability Certifications

We propose amending the rules to provide that any 911 Authorities are entitled to receive, upon request to the CSP, the annual reliability and interoperability certifications filed with the Commission directly from CSPs operating in their jurisdictions. Furthermore, we propose to adopt the same process for NORS access that state and local governments may follow for access to the 911 reliability and interoperability certificate system. Accordingly, 911 Authorities will have options for accessing 911 reliability and interoperability certification data, and may use the option that best suits their local needs and relationships with CSPs. We seek comment on these proposals.

Under existing rules, 911 reliability certifications are presumptively confidential.[183] The Commission adopted the rule in 2013 after balancing the interests of CSPs to protect proprietary and sensitive information and the public's access to 911 reliability information.[184] The Commission recognized that ''PSAPs and state 911 authorities have a strong interest in obtaining relevant information about the reliability and resiliency of their 911 service.'' [185] The Commission noted that PSAPs identified a limited set of information they believed to be important in assessing reliability of their service (*e.g.,* circuit audits), and accordingly, the Commission found no reason to address the need for disclosure of additional information to PSAPs and/or state 911 authorities.[186] Nonetheless, the Commission expected that CSPs ''will, at the request of the PSAP (or state 911 authority, as relevant), enter into discussions concerning the content of the provider's 911 circuit auditing certification with respect to the PSAP.'' [187] In light of the wide variety of circumstances involved in how PSAPs nationwide purchase 911 service, the Commission declined ''to require specific disclosure by rule, preferring to allow parties to negotiate reasonable and appropriate terms for assuring protection of proprietary information.'' [188] The Commission made clear, however, that CSPs ''should respond promptly to a PSAP request in this area'' and reiterated its belief ''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.'' [189]

We seek comment on whether there is an increased need for state and local government access to 911 reliability and interoperability certification data today, particularly in light of the advancing NG911 transition and the new roles being adopted by 911 Authorities and private network operators. Do other changes in network architecture evolution also change the need for state and local access to Commission data concerning 911 reliability and interoperability? For example in 2021, the Commission concluded that directly sharing NORS data with state and federal agencies, subject to appropriate and sufficient safeguards, is in the public interest, and the Commission extended this finding to include the sharing of DIRS data.[190] The

[179] 47 CFR 0.392(j) (''The Chief of the Public Safety and Homeland Security Bureau is delegated authority to . . . develop and revise forms and procedures as may be required for the administration of part 9, subpart H, of this chapter. . . .'').

[180] 47 CFR 0.392(h) (''The Chief, Public Safety and Homeland Security Bureau or her/his designee is authorized to issue non-hearing related subpoenas for the attendance and testimony of witnesses and the production of books, papers, correspondence, memoranda, schedules of charges, contracts, agreements, and any other records deemed relevant to the investigation of matters within the jurisdiction of the Public Safety and Homeland Security Bureau.'').

[181] 47 CFR 0.392(j) (''The Chief of the Public Safety and Homeland Security Bureau is delegated authority to . . . order remedial action on a case-by-case basis to ensure the reliability of 911 service in accordance with such rules and policies.'').

[182] 47 CFR 0.392(j).

[183] Specifically, Rule 0.457(d)(1)(viii) states: ''Information submitted with a 911 reliability certification pursuant to 47 CFR 12.4 [now 47 CFR 9.19] that consists of descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification elements, information detailing specific corrective actions taken with respect to certification elements, or supplemental information requested by the Commission with respect to such certification.'' 47 CFR 0.457(d)(1)(viii). *See* 47 CFR 9.19(d)(2)(i) and (ii).

[184] *911 Reliability Order,* 28 FCC Rcd at 17533, paras. 157–158.

[185] For example, NENA stated that ''PSAPs may be in the best position to use this information to prompt 911 service providers to make specific reliability improvements in their networks, but they may not otherwise be able to negotiate reliable access to this information through their contracts or tariffs.'' *911 Reliability Order,* 28 FCC Rcd at 17533, para. 157.

[186] *911 Reliability Order,* 28 FCC Rcd at 17533, para. 158.

[187] *911 Reliability Order,* 28 FCC Rcd at 17533, para. 158.

[188] *911 Reliability Order,* 28 FCC Rcd at 17533, para. 158.

[189] *911 Reliability Order,* 28 FCC Rcd at 17533, para. 158.

[190] *See NORS Information Sharing Order,* 36 FCC Rcd 6136. By way of background, the Commission collects network outage information in the Network Outage Reporting System (NORS) and infrastructure status information in the Disaster Information Reporting System (DIRS). This information is sensitive for reasons concerning national security and commercial competitiveness, and the Commission thus treats it as presumptively confidential. The Commission makes this information available to the Department of Homeland Security's (DHS) National Cybersecurity

Continued

Commission limited eligibility for direct access to our NORS and DIRS databases to ''need to know'' agencies acting on behalf of the federal government, the 50 states, the District of Columbia, Tribal Nations, and the U.S. territories.[191] In discussing sharing of complete NORS and DIRS reports and filings, the Commission noted ''that sympathy reports and reports containing information about TSPs contain actionable information on outages that could be of use to public safety officials for emergency response or service restoration and declined to exclude these reports from NORS filings. For example, sympathy reports contain information regarding service outages that, while caused by a failure in the network of another provider, nonetheless have an effect on the reporting service provider that may have public safety implications.'' [192]

Under our proposal, we would retain the existing requirements under § 9.19(d)(2)(i) and (ii), but would add that 911 Authorities will be eligible to accessing the 911 reliability and interoperability certification database under the same conditions as NORS access, and also require CSPs to provide their annual certifications to 911 Authorities in their CSP service areas upon the request of a 911 Authority.[193] For example, if a 911 Authority issues a request to contacts a CSP, including a CSP that delivers 911 traffic to the in-state NG911 Delivery Point, the CSP would be required to provide the information applicable to that 911 Authority and within that 911 Authority's jurisdiction. We believe that 911 Authorities have a strong interest in accessing certification filings to ensure the reliability of 911 traffic in their jurisdictions during the NG911 transition.[194] In addition, we believe 911 Authorities would benefit from having 911 reliability and interoperability certifications to assist with developing emergency response plans in advance of an outage.

We acknowledge that certifications are presumptively confidential under our existing rules, and CSPs and 911 Authorities must agree to confidentiality for sharing certifications. Under today's proposed approach, CSPs must share relevant portions of certifications, but may omit or redact information relating to portions of their networks that are not located within and not providing any service directly to the requesting 911 Authority's jurisdiction. CSPs may condition providing their certifications on the 911 Authority executing a confidentiality agreement.

We also propose extending our NORS/DIRS information sharing framework to 911 reliability and interoperability certifications to 911 Authorities only. 911 Authorities who prefer not to request confidential certifications directly from CSPs may request access to certifications from the Bureau under the same terms currently provided under rule 4.2.[195] CSPs receiving a request to provide a certification to a 911 Authority must provide it within 14 days under confidentiality terms no more restrictive than the same rule.[196] We seek comment on whether this proposal would best help ensure 911 Authorities' access to valuable information. Would this proposal incentivize cooperation between states and CSPs? Do 911 Authorities prefer having the option to seek this information either directly from CSPs or from PSHSB? We seek comment on this proposal and any alternatives.

Finally, we propose to amend § 9.19(d) of the rules to require CSPs to notify their 911 Authority of cessation of service at the same time they notify the Commission. Under our current rules, CSPs that cease covered operations under this section must notify the FCC by filing a notification under penalty of perjury no later than 60 days after the cessation of service.[197] For the reasons discussed above, we believe that 911 Authorities would benefit from having situational awareness of when CSPs cease providing services to their jurisdictions, and seek comment on this proposal, including alternatives, and potential costs to CSPs.

3. Remedial Action and Petition Process

To promote accountability and transparency in ensuring 911 reliability and interoperability, we propose to amend § 9.19 of the rules to add a new paragraph to provide guidance regarding the Bureau's process for responding to reliability and interoperability concerns. In addition, we seek comment on adopting a procedure for 911 Authorities to submit petitions alleging violations of the Commission's 911 reliability and interoperability rules to the Bureau, which then would have the option to exercise its authority under § 0.392(j) to launch investigations or direct remedial action against CSPs.[198]

Currently, § 0.392(j) references the Bureau's delegated authority to administer the 911 reliability rule and order remedial action for deficiencies, but § 9.19 does not explicitly reference the Bureau's delegated authority under 0.392(j).

To formalize the remediation order process, we propose to codify into the rules that when certification filings or other information available to the Commission indicate that a CSPs actions appear to be deficient or inadequate to address any of the risks to the reliability or resiliency of 911

and Communications Integration Center but does not share the information more broadly with other federal, state, or local partners. *New Part 4 of the Commission's Rules Concerning Disruptions to Communications,* ET Docket No. 04–35, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16856, para. 47 (2004), 69 FR 68859 (Nov. 26, 2004), 69 FR 70316 (Dec. 3, 2004) (making NORS reports available to DHS ''in encrypted form and immediately upon receipt'').

[191] *NORS Information Sharing Order,* 36 FCC Rcd at 6141, para. 16.

[192] *NORS Information Sharing Order,* 36 FCC Rcd at 6160, para. 78.

[193] In that connection, we would also retain the existing record retention requirements under 47 CFR 9.19(d)(3) with updates to cover interoperability certifications and streamlining as noted above.

[194] *See, e.g.,* Washington Utilities and Transportation Commission Comments, PS Docket No. 14–193, p. 8 (filed March 17, 2015) (''Additionally, as part of the cooperative framework with state and local partners the Commission seeks to maintain, the UTC suggests the proposed expanded certification requirements of Rule 12.4 be modified to require that all covered entities that submit annual certification, compliance, or audit reports, should also be required to simultaneously submit such information to designated state governance officials, such as the UTC and the Washington State E911 Coordinator's Office, that are actively involved or have some oversight responsibilities with respect to reliable 911 service delivery at the state level. 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, like the April 2014 multi-state outage, in understanding and interacting with such entities as events unfold. The UTC urges the Commission to modify the certification and reporting requirements of Rule 12.4 by requiring covered 911 service providers to submit certification and compliance information and reports to the Commission's state partners.'').

[195] 47 CFR 4.2.

[196] To protect sensitive communications status data, Participating Agencies and Downstream Agencies must preserve the confidentiality of certification filings. The Commission will grant access to certification filings only after 911 Authorities certify that they will comply with requirements for maintaining the confidentiality of the data and the security of the databases. 911 Authorities will also be responsible for ensuring downstream agencies certify that they, too, will maintain the confidentiality of the data they receive. *See* 47 CFR 4.2.

[197] 47 CFR 9.19(d)(4).

[198] 47 CFR 0.392(j) (''The Chief of the Public Safety and Homeland Security Bureau is delegated authority to administer the communications reliability and redundancy 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 certifications filed in connection therewith, and order remedial action on a case-by-case basis to ensure the reliability of 911 service in accordance with such rules and policies.'')

networks, the Bureau Chief or other Bureau official acting on the Chief's delegated authority will first issue and serve upon the CSP a notice that describes the apparent deficiencies and proposes different or additional actions that CSP must take to mitigate the apparent deficiencies. A CSP would have 30 days to submit a written response disputing the allegations and/or providing alternatives for remediation to such a notice. Any time after the 30th day a CSP receives notice from the Bureau, the Bureau may issue and serve upon the CSP an order setting forth its findings as to such deficiencies and specifying the actions that the CSP is required to take to mitigate the deficiencies. The order may specify deadlines by which the CSP must complete the required actions and may identify information that the CSP must submit to demonstrate its compliance with the order. We seek comment on this proposal.

Second, we propose to establish a process under which a 911 Authority may file a petition with the Bureau against a CSP in the 911 Authority's jurisdiction using alternative measures or claiming inapplicability in the certification, or for inaccurate certifications, alleging a lack of reasonable network practices in conformity with our rules. The petition process would be subject to the procedural requirements set forth in § 1.41 (informal requests for Commission action), 1.45 (pleadings and filing periods), and 1.47 (service of documents) of the rules.[199] Prior to filing a petition with the Bureau, a 911 Authority must provide the CSP with 30 days written notice to provide the CSP an opportunity to address the issue directly with the 911 Authority. If the issue has not been addressed to the 911 Authority's satisfaction within 30 days, the 911 Authority may file a petition with the Bureau Chief for relief no later than an additional 30 days later, and the 911 Authority's filing should include the relevant correspondence with the CSP and all documentation applicable to base a finding of lack of reasonableness. Petition proceedings will be treated as non-public restricted adjudicatory matters. CSP will have the proof burden to demonstrate their network practices and facilities are reasonable under rule 9.19(b), unless they have certified to meeting all benchmarks for their facilities, in which case the burden to show unreasonableness shifts to the petitioning 911 Authority. The petition must be in the form of an affidavit signed by the 911 Authority, and contain all relevant facts and references to this rule section alleging a violation. This proposal is similar to the petition process the Commission recently adopted for OSPs to challenge the validity of 911 Authorities' NG911 Phase 1 and Phase 2 requests.[200] We also propose to specify that 911 Authorities may continue to informally refer alleged 911 reliability and interoperability deficiencies to the Bureau without a formal petition.[201] We seek comment on these proposals.

We invite comment on whether our proposals will promote transparency and accountability to 911 Authorities and assist 911 Authorities with local oversight. Will these proposals incentivize greater collaboration between 911 Authorities and CSPs, and serve as a backstop should 911 Authorities and CSPs reach an impasse? We invite comment on our proposals, including potential alternatives and costs on CSPs and 911 Authorities. Do commenters perceive risks in establishing that 911 Authorities contact CSPs to address reliability and interoperability concerns before filing a report with the Bureau, and encouraging 911 Authorities and providers to resolve such issues before contacting the Bureau? We seek comment on establishing such a step in our process.

Regarding providing CSPs with notice of potential Bureau remediation inquiries or orders under § 0.392(j) of our rules, do commenters agree with adopting formal procedures for Bureau actions specifying the process and time for CSPs to respond to an inquiry? We seek comments on what procedures CSPs should follow in such a process. Thus, we seek comment on whether our proposed rule would add another layer of transparency and oversight regarding the Bureau's processes to ensure CSPs are accountable for reliability and interoperability measures. We invite comment on the potential costs and risks associated with our proposal.

E. Legal Authority

We tentatively conclude that the rules we are proposing in this FNPRM are well-grounded in our broad authority to ''promot[e] safety of life and property through the use of wire and radio communications,'' [202] including through use of the nation's 911 system.[203] Congress has enacted numerous provisions in the Communications Act and other 911-related statutes ''that, taken together, establish an overarching federal interest in ensuring the effectiveness of the 911 system.'' [204] Beyond this general mandate, section 251(e)(3) of the Communications Act confirms the Commission's authority and responsibility for designating 911 as the universal emergency telephone number for both wireline and wireless telephone service,[205] demonstrating Congress's intent to grant the Commission broad authority for ''ensuring that 911 service is available throughout the country.'' [206] 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

[199] 47 CFR 1.41, 1.45, and 1.47.

[200] 47 CFR 9.31(c).

[201] *See* Public Safety Support Center at *https://www.fcc.gov/general/public-safety-support-center* (last visited Feb. 14, 2025).

[202] 47 U.S.C. 151. The Communications Act of 1934, as amended (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), 303(r).

[203] *See, e.g., Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems; Amendment of Parts 2 and 25 to Implement the Global Mobile Personal Communications by Satellite (GMPCS) Memorandum of Understanding and Arrangements; Petition of the National Telecommunications and Information Administration to Amend Part 25 of the Commission's Rules to Establish Emissions Limits for Mobile and Portable Earth Stations Operating in the 1610–1660.5 MHz Band,* CC Docket No. 94–102, IB Docket No. 99–67, Report and Order and Second Further Notice of Proposed Rulemaking, 18 FCC Rcd 25340, 25345, para. 13 (2003), 69 FR 6578 (Feb. 11, 2004), 69 FR 6595 (Feb. 11, 2004) (''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), 59 FR 54878 (Nov. 2, 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). *Nuvio Corp.,* 473 F.3d at 312 (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.*

[204] *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), 86 FR 45892 (Aug. 17, 2021) (*911 Fee Diversion Order*); *NG911 Transition Order* at *52, para. 154.

[205] 47 U.S.C. 251(e)(3).

[206] *Nuvio Corp.,* 473 F.3d at 311 (Kavanaugh, J., concurring).

capabilities possible should be available to all citizens in all regions of the Nation.'' [207] 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 public interest.[208] 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.

Moreover, to the extent that 911 service providers are common carriers, section 201(b) of the Communications Act requires the providers 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.[209] 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.'' [210] The Commission consistently has relied on these authorities before to regulate the provision of 911 service, including when it adopted the reliability rules we propose to modify today.[211] Similar provisions empower the Commission to regulate the adequacy of the services provided by wireless and interconnected VoIP providers.[212]

We believe that the Commission also has broad authority under the Twenty-First Century Communications and Video Accessibility Act (CVAA) to regulate the provision of NG911 services specifically.[213] 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[.]'' [214] 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].'' [215] Importantly, 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.'' [216] Ensuring the reliability and interoperability of the nation's NG911 network therefore is one of the Commission's key mandates under the CVAA.

We believe the rules we propose today comport with the CVAA's mandate because they would enhance the reliability and interoperability of the nation's NG911 network—the IP-enabled emergency network addressed in the CVAA. The proposed rules would: (1) clarify and expand the definition of ''covered 911 service providers'' so that the facilities that are most critical to modern NG911 networks are subject to reliability standards; (2) require basic interoperability between ESInets; and (3) improve the process for covered 911 service providers and ESInets to certify their reliability and interoperability. These amendments are intended to reduce NG911 service outages, thereby increasing access to IP-based 911 services for people with disabilities, including through the use of internet-based TRS, which is used primarily by persons who are deaf, hard of hearing, deafblind, or have a speech disability, as well as through the use of wireline, CMRS, covered text, and interconnected VoIP services with multimedia capabilities that cannot be supported on legacy TDM-based networks.[217] 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.'' 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 interoperability rules we have proposed. 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[.]'' That is the approach we are proposing to take.

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.[218] Nor does the CVAA ''requir[e] the FCC to ensure that any rules we adopt confer zero benefits on consumers outside the disability community[.]'' [219] Rather, we believe the rules we propose today would adhere to and advance the CVAA's mandate precisely because they would promote NG911 reliability equally between people with and without disabilities on a platform-neutral basis. Moreover, the EAAC concluded that, in emergency situations, people with disabilities may

[207] ENHANCE 911 Act of 2004, Public Law 108–494, § 102, 118 Stat. 3986, 3986 (2004) (codified at 47 U.S.C. 942 note).

[208] *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'').

[209] 47 U.S.C. 201(b).

[210] 47 U.S.C. 214(d).

[211] *See, e.g., 911 Reliability Order,* 28 FCC Rcd at 17529, para. 149.

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

[213] Twenty-First Century Communications and Video Accessibility Act of 2010, Public Law 111–260, 124 Stat. 2751 (2010).

[214] 47 U.S.C. 615c(a).

[215] 47 U.S.C. 615c(c), (g).

[216] 47 U.S.C. 615c(g).

[217] *See* Emergency Access Advisory Committee (EAAC), Report and Recommendations, at 21–25 (Dec. 7, 2011), *http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-312161A1.doc* (describing NG911 functions that can benefit persons with disabilities) (*EAAC Report*).

[218] *NG911 Transition Order* at *53, 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), 78 FR 32169 (May 29, 2013) (''[T]he FCC has authority under the CVAA to require action that is not limited to the disability community.'') (*Bounce-Back Order*); *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), 79 FR 55367 (Sept. 16, 2014), 79 FR 55413 (Sept. 16, 2014) (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'') (*T911 Second Report and Order*).

[219] *T911 Second Report and Order,* 29 FCC Rcd at 9878, para. 71.

depend on the same wireline, CMRS, covered text, and interconnected VoIP services as those without disabilities,[220] or they may rely on a caretaker or other persons using such services.[221] We believe the Commission's NG911 rules therefore should broadly cover different types of service providers in order to ensure that persons with disabilities will have full and equal access to emergency services when they are needed.

In addition to the CVAA, we believe that the other 911-related statutes discussed above confirm the Commission's authority and responsibility to establish and maintain a comprehensive and effective 911 system.[222] Together, the statutes 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 rules proposed herein; and represent the repeated endorsement by Congress of the Commission's ability to act in this context.[223] 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.'' [224] The Commission also has stated that ''[t]he Commission 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.[225]

With respect to our proposals to amend the reliability certification process and to allow 911 Authorities to request relevant certifications, we note that section 218 of the Communications Act authorizes 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.'' [226] Furthermore, section 4(n) of the Communications 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.'' [227] The Commission has previously 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.[228] The Commission also has authority under the NET 911 Act to ''compile . . . 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.'' [229] Thus, 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.'' [230] We seek comment on the foregoing legal analysis.

We also note that our proposals do not seek to alter state jurisdiction over 911 or directly affect intrastate facilities. Rather, we propose to empower 911 Authorities by ensuring them access to the reliability certifications of service providers in their states and creating an optional process by which 911 Authorities can choose to address rules violations to the FCC. We also specifically propose to exempt PSAPs and other governmental entities from the reliability obligations we propose today while focusing on the interstate paths within multistate 911 networks that no individual state can regulate effectively. Similarly, the ESInet interoperability requirement we would adopt also applies only to interstate communications. Consistent with past practice, we intend to implement our proposals in partnership with state, territorial, Tribal, and local authorities while respecting their unique interest in the delivery of 911 service to their communities. We seek comment on additional considerations for striking the most effective balance between state and federal authority to ensure the reliability and interoperability of the nation's NG911 network.

F. Benefits and Costs

Benefits. To estimate benefits of today's proposals, we rely on our calculation of the benefit of improved 911 reliability in the *NG911 Transition Order.*[231] The Commission has previously relied on a study examining 73,706 emergency incidents in the Salt Lake City area that found that, on average, a one-minute decrease in ambulance response times would reduce the total number of post-incident deaths from 4,386 deaths to 3,640 deaths within 90 days after the incident (746 lives saved), representing a 17% reduction in mortality.[232] According to

[220] *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.'').

[221] *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.'').

[222] *911 Fee Diversion Order,* 36 FCC Rcd at 10810–11, para. 16 (stating that federal 911-related statutes and the Communication Act's provisions ''establish an overarching federal interest in ensuring the effectiveness of the 911 system'').

[223] *Id.* at 10810–11, para. 16.

[224] *911 Reliability Order,* 28 FCC Rcd at 17529, para. 150.

[225] 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.'').

[226] 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'').

[227] 47 U.S.C. 154(n).

[228] *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), 89 FR 2503 (Jan. 16, 2024) (citing *The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to 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), 77 FR 25088 (Apr. 27, 2012)).

[229] 47 U.S.C. 615a–1(g).

[230] *2014 Reliability NPRM,* 29 FCC Rcd at 14235, para. 78.

[231] *NG911 Transition Order* at **63–64, **66–67, paras. 185–86, 194–96.

[232] *See* Elizabeth Ty Wilde, *Do Emergency Medical System Response Times Matter for Health Outcomes?,* 22(7) Health Econ. 790–806 (2013), *http://www.ncbi.nlm.nih.gov/pubmed/22700368* (*Salt Lake City Study*). The study examined 73,706 emergency incidents during 2001 in the Salt Lake City area. *Id.* at 794. The study found that the one-minute increase in response time caused mortality to increase 17% at 90 days past the initial

Continued

the National Association of State Emergency Medical Services Officials (NASEMSO), local Emergency Medical Services (EMS) agencies respond to nearly 28.5 million 911 dispatches each year.

We assess that improvements to 911 reliability from the proposed rules will reduce 911 call failures and outages. We estimate that, from 2019 through 2023, an average of 4.1 billion user-hours of telecommunication voice service outages per year were reported to the Commission.[233] If these 4.1 billion user-hours of outages were distributed evenly across the total U.S. population (approximately 335 million people),[234] this is equivalent to each person in the country experiencing an average of 12 hours of voice telecommunications service outages per year.[235] Hence, we estimate that on average, consumers experience telecommunications outages 0.14% of the time per year.[236] As noted above, available evidence shows that 911 calls resulted in 28.5 million EMS dispatches per year during the most recent year when data was available. If service outages prevent 0.14% of these 911 calls from going through, that means 39,900 potentially life-saving emergency 911 calls would be dropped per year as a result of legacy 911 system failures.[237]

If we conservatively estimate that our proposed rules improving 911 reliability reduce the number of 911 outages and call failures by just 1%, this will translate to a reduction in mortality risks associated with emergency medical situations for which ambulances were dispatched in response to 911 calls roughly equivalent to 23 lives saved per year.[238] While we do not attempt to place a value on human life, we note that the amount consumers are willing to pay to reduce mortality risk is approximately $13.2 million, using a methodology developed by the U.S. Department of Transportation (DOT) that the Commission has relied on in past orders.[239] We seek comment on this benefits estimate.

Costs—Initial Considerations. As the Commission observed in the *NG911 Transition Order* and as remains similarly true here, many of the proposed reliability rules describe network changes which providers are already implementing due to factors independent of any rules the Commission ultimately might adopt as a result of this FNPRM.[240] The transition to IP networks broadly and to NG911 networks in particular naturally has the capacity to increase 911 reliability, partly due to the fact that IP reliability measures are a standard industry best practice from a quality-of-service standpoint.[241] Provider concerns about various liabilities or risks to their business as a consequence of 911 outages preventing people from reaching 911 will also cause network operators to independently implement the measures we propose today.[242] Finally, the Commission has already assessed the costs of transitioning to IP-based 911 facilities with their greater inherent reliability in the *NG911 Transition Order.*[243] Accordingly, we assess that any additional cost impact of today's proposed rules will be limited in light of the independent factors of technological advancement, ordinary market forces, and prior Commission actions, all of which will accomplish a substantial portion of the reliability and interoperability improvements we seek today for certain networks.

Furthermore, in calculating these costs, we emphasize that the only affirmative operational requirement we propose today is for network reliability practices to be *reasonable.* The specific benchmarks we propose for path physical diversity, network monitoring, and operational integrity are merely measures we have identified which—if network operators meet them for critical facilities—presumptively demonstrate

---

incidence, *i.e.,* an increase of 746 deaths, from a mean of 4,386 deaths to 5,132 deaths. *Id.* at 795. Because the regression is linear, this result implies that a one-minute reduction in response time also saves 746 lives, *i.e.,* a 17% reduction from a mean of 4,386 deaths to 3,640 deaths. *NG911 Transition Order* at *66, para. 193, n.569 (''The Salt Lake City Study shows a one-minute decrease in ambulance response times reduced the likelihood of 90-day mortality from approximately 6% to 5%, representing a 17% reduction in the total number of deaths.'').

[233] We estimate the average time consumers were affected by outages was approximately 4.1 billion user-hours per year based on data from the Commission's Network Outage Reporting System (NORS) between 2019 and 2023. Staff calculation. FCC, *Network Outage Reporting System (NORS)* (Nov. 30, 2023), *https://www.fcc.gov/network-outage-reporting-system-nors.*

[234] *See* U.S. Census Bureau, *National Population Totals and Components of Change: 2020–2023* (Dec. 18, 2023), *https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-total.html* (*Census Population Estimates*) (referring to Annual Estimates of the Resident Population for the United States, Regions, States, District of Columbia and Puerto Rico: April 1, 2020 to July 1, 2023 (NST–EST2023–POP) on the page, which estimates U.S. population around 334,914,895 as of July 1, 2023).

[235] We calculate the average outages a U.S. resident experience as follows: 4.1 billion user-hours/335 million residents = 12.24 hours per resident, which we round to 12 hours.

[236] We estimate the average percentage of time U.S. consumers experience telecommunication network outages as follows: average 12.24 hours of outages/(24 hours per day × 365 days per year) = 0.14% outage per year.

[237] We estimate the life-threatening emergency 911 calls that would be dropped due to call failures or system outages as: 28.5 million EMS dispatches × 0.14% outages = 39,900 potentially life-saving emergency 911 calls dropped per year.

[238] A 1% reduction in call failures results in 23 lives saved (39,900 dropped calls per year × 1% reduction in call failures × 5.95% (90 day mortality in *Salt Lake City Study*) = 23.74, rounded down to 23). Note that this calculation conservatively equates a dropped call with an approximately 3.5-second savings in response time based in the *Salt Lake City Study.* The study finds that the one-minute increase in response time caused mortality to increase 17% at 90 days past the initial incidence, meaning that a 3.5-second increase in response time would cause a 1% (roughly 3.5/60 × 17%) mortality increase.

[239] *See NG911 Transition Order* at *66, para. 194, n.574; U.S. Department of Transportation, *Departmental Guidance on Valuation of a Statistical Life in Economic Analysis* (May 7, 2024), *https://www.transportation.gov/office-policy/transportation-policy/revised-departmental-guidance-on-valuation-of-a-statistical-life-in-economic-analysis*). Twenty-three estimated lives saved per year times the 2023 value of $13.2 million is approximately $304 million per year. *See NG911 Transition Order* at *67, para. 195, n.580 (calculating 23 lives saved per year from increased 911 system reliability).

[240] *See e.g. NG911 Transition Order* at *72, para. 209 (''Although we agree that converting TDM networks to IP networks can be costly, we reject the contention that such system upgrade costs should be attributed to the requirements in these rules. The transition from TDM to IP technology has been ongoing for over a decade as the subscriptions to voice-only local exchange telephone service (switched access lines) has fallen from nearly 141 million lines in December 2008 to 27 million in June 2022. A linear model predicts that switched access lines will be fully phased out in the near future. Therefore, since we can reasonably expect that these system upgrades will occur organically as part of the natural technological evolution, regardless of whether OSPs are required to comply with Phase 2 requests, the cost of the upgrades cannot be attributed to these requirements. Instead, they should be considered baseline costs of operating telecommunications business.'').

[241] *NG911 Transition Order* at *64, para. 186 (''[T]he more extensive use of IP routing in the Phase 2 architecture is inherently more reliable than legacy TDM selective routing because of the greater capability of IP traffic to be dynamically rerouted among various available paths.'').

[242] *NG911 Transition Order* at *59, paras. 172, 174 (''RLEC commenters express concern that they will face increased liability costs for 911 call failures occurring within the networks of the third-party transport services they will retain to deliver 911 calls beyond their service areas . . . .'' However, ''the implementation of NG911 is far more likely to reduce the risk of dropped 911 calls than to increase it. OSPs that make the necessary changes to fully implement NG911 will be able to leverage improvements to 911 security and reliability, including the ability to reroute 911 calls in response to network congestion or outages. Indeed, OSPs may face greater exposure to liability due to the risk of dropped 911 calls if they fail to implement NG911 in a timely and prudent manner as the NG911 rules require.'').

[243] *NG911 Transition Order* at *61–62, paras. 180–81 (estimated benefits from 911 improvement to reduction in mortality of approximately $617 billion over ten years, and costs of approximately $321 million over ten years). *See also NG911 Transition Order* at *26, *28, paras. 71, 78 (describing OSP's NG911 Phase 1 and Phase 2 technology deployment obligations triggered by a 911 Authority's transition readiness request); 47 CFR 9.29 (same).

reasonableness. Networks can continue to use alternative measures that they certify are reasonable to ensure reliability. Accordingly, no network will be required to meet our benchmarks for their critical facilities even if we adopt today's rule proposals. We are not proposing to change the fundamental structure of the 911 reliability regulation, which requires a separate and subsequent Bureau inquiry and finding of an unreasonable network practice in a Remediation Order prior to imposing costs. Such a Remediation Order would require its own separate weighing of the costs and benefits for any targeted directive to improve the reliability of specific network facilities, and that analysis must stand on its own. Today we propose to preserve a regulatory structure that was already adopted in 2013 and was found at that time to have substantial benefits which greatly outweighed the limited costs.[244] In sum, the only potential costs of today's item would be to those covered network operators that are failing to take measures widely deemed ''reasonable'' by industry standards, including reasonable interoperability. Accordingly, we estimate that the costs of these proposed regulations on their own is not substantial. We further assess that, to the extent commenting parties estimate that the costs are substantial, this would indicate a higher level of unreasonableness or negligence on the part of private entities operating the nation's critical 911 call traffic bottleneck facilities than we currently estimate.

Finally, today's proposals leave the 2013 best-practice benchmarks for legacy 911 circuits, monitoring, and backup power in place, imposing no new obligations on entities operating legacy 911 facilities. Moreover, the reasonableness obligation has always applied to NG911 facilities in certain central offices or with direct contractual relationships with 911 Authorities or PSAPs through the ''functional equivalent'' and ''equivalent NG911 facilities'' language in the current rules.[245] Accordingly, we view the impact of today's changes even on NG911 network facilities to be minimal. Further, we observe that most of any potential new cost impact would apply to NG911 networks and facilities, many of which are in the process of being designed and constructed, and which—given NG911's inherent increased reliability[246]—would mostly be constructed with the specified benchmarks we articulate today.

Nevertheless, despite the fact that these rules reflect steps that providers will undertake as an ordinary baseline cost of doing business, the fact the rules require only reasonableness and do not dictate substantial investment in specific technologies, and the likely minimal impact to both legacy TDM and NG911 IP critical facilities, we will err on the side of conservatism and estimate the following network cost elements as a potential impact of today's proposals.

Anticipated Affected Entities. 290 entities filed 911 Reliability Certifications in 2024. The large majority of these entities filed to certify legacy 911 facilities only, with a smaller group certifying for NG911 equivalent facilities. We anticipate that, over the estimated five years of the NG911 transition,[247] the overall number of CSPs will shrink as smaller RLEC CSPs exit direct contractual 911 services to state and local government and retire their legacy 911 facilities of selective routers, TDM CAMA trunks, and ALI/ANI databases,[248] leaving other entities as the critical bottleneck facilities providers in the NG911 ecosystem.[249] Indeed, as of today, multiple previously-covered RLECs have already notified the Bureau that they have ceased providing the services of a CSP.[250] We estimate that this new smaller group of mostly larger national or regional providers will provide most of the specialized critical bottleneck facilities in the NG911 environment, including ''LIS as a service'' provided to OSPs,[251] major transport facilities,[252] VoIP Positioning Centers and traffic aggregation facilities,[253] and LNG facilities at the NG911 Delivery Point.[254] We anticipate

[244] *911 Reliability Order,* 28 FCC Rcd 17500–01, paras. 73, 75 (conservatively underestimating a life-saving mortality reduction benefit from the 911 improvements of *at least* one life per year, for a minimum statistical economic impact of $9.1 million *annually,* which easily outweighed the estimated maximum one-time costs of approximately $9 million *total*).

[245] 47 CFR 9.19(a)(4)(i)(A) and 9.19(a)(4)(i)(B).

[246] *NG911 Transition Order* at *63, para. 185 (''. . . NG911 will reduce the likelihood of 911 service outages because it will facilitate deployment of new facilities to replace the aging and failure-prone infrastructure used to operate the legacy 911 system.'').

[247] *NG911 Transition Order* at *61, para. 180, n.533 (''We estimate that, nationwide, both NG911 transition phases will be complete within five years, due in significant part to the provisions of this Order that remove obstacles to completion of the transition, but this estimate is quite conservative because the full transition will likely be completed sooner in many states and regions.'').

[248] *NG911 Transition Order* at *64, para. 186 (''Today's rules will accelerate the full retirement of the legacy TDM-based 911 system and facilitate use of an NG911 architecture that uses newer and less failure-prone facilities. Selective routers will be replaced with NGCS IP routing at the ESInet, ALI/ANI databases will be replaced with IP-based systems with more precise location information, TDM trunks will be replaced with IP transmission to provide faster connections, and traffic will be routed to more reliable and efficient IP-based NG911 Delivery Points'').

[249] *NG911 Transition Order* at *59, para. 174 (''[C]ertain commenters suggest that we should apply 911 network reliability and PSAP outage notification requirements to additional categories of service providers in an NG911 environment.''); *NG911 Transition Order* at *69 para 202 (''. . . OSPs could significantly lower the overall costs of transmitting 911 calls to ESInets by taking advantage of third-party aggregators' services.''); *See also* Home Telephone Comments, PS Docket 21–479, at 4–7 (filed Aug. 9, 2023) (new NG911 Service Providers will assume most responsibility for NG911 critical architecture but are currently unregulated by the Commission, as they are not required to comply with the Commission's 911 reliability reporting rules); NTCA Reply Comments, PS Docket 21–479, at 7–8 (filed Sept. 8, 2023).

[250] 47 CFR 9.19(d)(4); *See also PSHSB Announces Compliance Date and Instructions for Information Collection Requirement Associated with Improving 911 Reliability,* Public Notice, DA 24–524, PS Docket Nos. 15–80 and 13–75, p. 1 (PSHSB June 4, 2024) (''Beginning July 4, 2024 . . . notifications of cessation of operations should be filed with the Bureau staff via email to *911reliabilitycertification@fcc.gov*.''), at *https://docs.fcc.gov/public/attachments/DA-24-524A1.pdf.*

[251] *NG911 Transition Order* at *71, para. 206 (''CSRIC explains that LIS as a service is contemplated as an NG911 solution at 'minimal expense' to small OSPs, as it relieves OSPs of most costs beyond monthly services, and an LNG and can be provided either by a commercial vendor or the 911 authority.''); *NG911 Transition Order* at * 72, para. 208 (''AT&T, in its role as the lead NGCS and ESInet contractor in Virginia, has already provided a solution that allows legacy OSP wireline ALI and MSAG location data to be used for NG911–compliant LIS as a service, which eliminates TDM OSPs' needs to upgrade their networks to IP.'').

[252] *NG911 Transition Order* at *59, para. 174. *See also* Home Telephone Comments,, PS Docket 21–479, at 5 (filed 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 iii (''[T]he Commission should focus on the back-end for-profit entities that aggregate front-end 911 transmissions from multiple jurisdictions, process, and then deliver via back-end connections IP-based information to the appropriate local [PSAPs]. 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.''); USTelecom Comments, PS Docket 21–479, at 5 (filed Aug. 9, 2023); Windstream Reply Comments, PS Docket 21–479, at 2–3 (filed Sept. 8, 2023).

[253] *See* Inteliquent Reply Comments, PS Docket 21–479, at 1 (filed Sept. 8, 2023) (''Sinch provides a Voice over internet Protocol ('VoIP') Positioning Center ('VPC') service to VoIP providers. Sinch's VoIP customers contract with Sinch to facilitate VoIP 911 call delivery to the appropriate Public Safety Answering Points ('PSAP').''); *see also* Bandwidth Comments, PS Docket 21–479, at 2–3 (filed Aug. 9, 2023) (''Bandwidth predominately acts as a VoIP Positioning Center ('VPC') where it provides stand-alone emergency location and 911 call routing capabilities for its VoIP service provider customers . . . . Bandwidth has a robust network that reaches across the United States and Canada and delivers around 3 million calls a year from 26.7 million end points . . . . To date, Bandwidth established network aggregation capabilities to route its customers' 911 traffic through 16 ESInets.'').

[254] 47 CFR 9.33(a)(2) (OSPs are responsible for the bearing the costs of ''IP Conversion using a Legacy

Continued

these larger entities will provide critical 911 facilities and services on a contract and for-hire basis to the larger group of approximately 2,200 OSPs offering 911 call origination service to the public.[255]

Based on the foregoing, we tentatively estimate that the 911 reliability rule amendments we propose today will apply to approximately 100 larger entities, most of which are currently subject to the existing reliability rules for providing NG911 equivalent services. We further estimate that, of those entities currently providing only legacy 911 critical facilities, most will phase out in approximately 5 years and revert to providing 911 call origination services only, surrendering CSP status but otherwise remaining subject to the ''911 call transmission'' obligations and liability standard for originators.[256] We seek comment on this estimate.

Finally, we estimate that most of the benchmarks articulated here would already apply to covered entities providing NG911 equivalent services, because the majority of those providers are already subject to the reasonableness requirement which must be met with either alternative measures or the current articulated best practices. Furthermore, we assess that the new benchmark practices described today are standard IP network reliability measures that are generally being implemented as baseline costs for communications networks to meet expected quality of service standards, and so will only result in new costs to a few CSPs. In addition, because these rules impose a reasonableness requirement only, with safe harbor benchmarks that are mandatory obligations, we anticipate the cost impact will be even more narrow. Accordingly, we estimate that the changes to the rule would impact the network decisions of no more than one-quarter of these 100 entities, or 25 entities total. We seek comment on this estimate as well.

Critical IP Path Diversity for Major Transport Providers and IP 911 Aggregators. The primary cost for ensuring IP path diversity is redundancy of routers capable of load-balancing and automatic re-routing. We conservatively estimate the cost of such network routers at approximately $40,000 each.[257] Assuming 25 CSPs acquire new redundant routers to meet the proposed IP path diversity benchmark, the total cost would be approximately $1 million. We seek comment on this estimate.

To the extent CSPs must acquire additional IP transport to ensure diverse paths in and out of their facilities, we rely in part on our estimates of IP transport in the *NG911 Transition Order.*[258] We assess that most CSPs affected by today's proposals will be larger providers that are already aggregating or transporting aggregated NG911 IP traffic over SIP trunks with diverse and redundant paths.[259] We conservatively estimate that additional IP transport to connect to third-party networks will not exceed $3,000 per month relying on record evidence from the NG911 proceeding.[260] Furthermore, to the extent any CSP must acquire dedicated long-haul transport or SIP trunking, we rely on record evidence that such costs would be approximately $7,000 per month.[261] Conservatively estimating that 25 entities will acquire both additional last-mile transport and long-distance transport in response to our proposed rules, the estimated cost would be $3 million annually.[262] We seek comment on this estimate.

Furthermore, while the aggregated 911 traffic circuits of CSPs providing direct service to PSAPs have always been covered critical facilities under our rules, out of an abundance of caution, we include an estimate here, relying on the calculation in the *2013 Reliability Order.*[263] There, the Commission estimated that the total incremental cost of the critical circuit auditing and tagging best practice for all critical 911 circuits was $6.4 million annually.[264] We estimate less than a quarter of these critical legacy 911 circuits are impacted given that the previous record indicates ''only a segment of critical 911 circuits are not already subject to regular audits,'' [265] so any incremental cost would not exceed $2.4 million annually after adjusting for inflation.[266] We seek comment on this estimate.

Operational Integrity for LIS and LNG. We estimate the costs of meeting this benchmark would include servers, UPS devices, and collocation space. Based on data in the NG911 proceeding, we conservatively estimate the cost of diverse LNG or LIS servers at approximately $5,000 each.[267] We

---

Network Gateway or the functional equivalent, if necessary''); *NG911 Transition Order* at *49, para. 145, n.425 (''. . . OSPs also are responsible for the cost of the hardware and software components needed to transform TDM transmissions into the appropriate IP-based format (if necessary) . . . . At Phase 1, these components will typically include LNG facilities . . . .''); *NG911 Transition Order* at *51, para. 151 (''At Phase 1, our rules require OSPs to deliver 911 traffic in the IP-based SIP format requested by the 911 Authority, using either IP origination or IP translation through an LNG or other solution.''); *NG911 Transition Order* at *45, para. 132 (''. . . OSPs must transmit and deliver 911 traffic to NG911 Delivery Points designated by 911 Authorities and must bear the financial responsibility for such transmission, including costs associated with completing any needed TDM-to-IP translation . . . .'').

[255] *NG911 Transition Order* at *68, para. 198, n.588 (''Based on FCC Form 477 data as of June 2023, there are a total of 2,287 OSPs . . . .'').

[256] *See* 47 CFR 9.4, 9.10(b), and 9.11(a)(2)(ii).

[257] *See* ''NetMode,'' network router cost quotes of $18,295 (*https://netmode.com/product/new-cisco-ncs-5001-ncs-5001-series-router-ncs-5001-bun,* of $72,995 (*https://netmode.com/product/juniper-ptx10003-80c-ac-80x100ge-16x400ge-port-ac-or-dc-router-new*), and of $30,995 (*https://netmode.com/product/new-cisco-systems-asr1002-x-5g-vpn-bundle-asr1002x-5g-vpnk9/*) (last visited Feb. 14, 2025); *See also FCC Announces Final Supply Chain Reimbursement Program Procedures,* Public Notice, DA 21–947, WC Docket No. 18–89, 36 FCC Rcd 12190, 12255 (WCB 2021), 86 FR 48521 (Aug. 31, 2021) (identifying Multiprotocol Label Switching L3 router cost at $4,500).

[258] *NG911 Transition Order* at *69, paras. 200–202.

[259] Based on FCC Form 477 data as of June 2023, there are a total of 2,287 OSPs. Of the 291 large OSPs that serve more than 10,000 subscribers each, there are only 2 wireline OSPs that do not offer any form of IP services (*e.g.,* broadband or VoIP services), 20 wireline OSPs that also provide broadband services, 232 VoIP OSPs, and 37 wireless OSPs which provide IP services. Staff Calculation. FCC Form 477 Data as of June 2023. *See also* Jessica Dine and Joe Kane, *The State of US Broadband in 2022* (Dec. 5, 2022) (''4G covers almost 100 percent of the population.''), *https://itif.org/publications/2022/12/05/state-of-us-broadband-in-2022-reassessing-the-whole-picture/;* TechTarget, *What is 4G (fourth-generation wireless)?* (''4G is also an all-IP (internet protocol)-based standard for both voice and data . . .''), *https://www.techtarget.com/searchmobilecomputing/definition/4G* (last visited Feb. 14, 2025).

[260] *See NG911 Transition Order* at *69, para. 201 (staff estimated the transport cost would be $3,000 per month for OSPs that currently only offer TDM-based voice services, which should be treated as an upper bound for in-state transport cost).

[261] South Carolina Revenue and Fiscal Affairs Office Comments, PS Docket 21–479, at 4–5 (filed Aug. 8, 2023) (stating that the network transport costs to deliver SIP traffic from South Carolina to two delivery points in Dallas, Texas and Raleigh, North Carolina are $172,000 per year). This amounts to $86,000 per path, or approximately $7,000 per month.

[262] Total IP transport costs = ($3,000 + $7,000) per month × 12 months × 25 entities = $3 million per year.

[263] *911 Reliability Order,* 28 FCC Rcd at 17510–14, paras. 100–105.

[264] *911 Reliability Order,* 28 FCC Rcd at 17513, para. 103.

[265] *911 Reliability Order,* 28 FCC Rcd at 17512, para. 102. *See also 2013 Reliability Order,* 28 FCC Rcd at 17511, para. 101 (most CSPs ''already perform regular diversity audits for many . . . critical 911 circuits'').

[266] We estimate a 146% inflation adjustment between December 2013 and September 2024. *See* Federal Reserve Bank of St. Louis, *Average Hourly Earnings of All Employees, Total Private (CES0500000003), https://fred.stlouisfed.org/series/CES0500000003* (last visited Feb. 14, 2025) (*Inflation Adjustment*) (showing that the average hourly private wage increased from to $35.36 in September 2024, approximately 146% of the average hourly wage of $24.18 in December 2013). Therefore, we estimate the total cost as $6.4 million × (1/4) × 146% = $2,336,000, rounded to $2.4 million.

[267] Brian Rosen Reply Comments, PS Docket 21–479, at 2 (filed Sept. 8, 2023) (''The RLECS commenting on this proceeding wildly overestimate the cost of the gateway required to convert TDM to

further estimate the cost of uninterruptible power supply or UPS devices on the high-end of approximately $3,000 per unit.[268] Finally, we conservatively estimate the cost of any needed diverse secondary server collocation ''full rack'' space at approximately $700 per month.[269] Collectively, assuming the same 25 entities would acquire this reasonable reliability—and would not have done so absent today's proposals—this amounts to $200,000 in one-time costs and recurring cost of $210,000 annually.[270] We seek comment on this estimate.

IP Network Monitoring. We estimate the costs of IP network monitoring capability as similar in facilities as those of operational integrity for LIS and LNG. Accordingly, we start with the same $200,000 in one-time costs and $210,000 annually as an impact of this proposal. However we add an additional estimated $2,000 per year in monitoring software licensing costs,[271] which we multiply by 25 estimated entities to $50,000, for a total to $260,000 annually. We seek comment on this estimate.

Interoperability. We tentatively estimate the costs of acquiring interoperability capability as substantially similar to those of IP network monitoring. Accordingly, we tentatively estimate $200,000 in one-time costs and $260,000 annually as an impact of this proposal. We seek comment on this estimate.

Labor Costs—Software, Engineering, and Installation. We estimate additional labor costs for programming, engineering, and installation for integrating and/or testing each of the above reliable and interoperable facilities. Assuming the average wage of a software developer is $63.75/hour,[272] with a 45% markup for benefits,[273] we arrive at $92.44/hour as the compensation rate for software developers. Assuming the average wage of computer network engineers is $54.95/hour,[274] with a 45% markup for benefits, we arrive at $79.68/hour as the compensation rate for network engineers. We also assume the average benefits-adjusted wage for telecommunications equipment installers and repairers is $46.78 per hour.[275]

We tentatively estimate additional labor costs of meeting benchmarks not already implemented would be approximately 160 labor-hours total in each of those three categories. Accordingly, the estimated labor costs would be approximately $14,790 in software labor, $12,748 in engineering labor, and $7,484 in installation labor, for a total of $35,023 per CSP. Estimating the same figure of 25 CSPs that will newly decide to begin meeting the reasonableness benchmarks as a result of today's proposed rules, the total estimated one-time labor cost is $875,568. We seek comment on this estimate.

Labor Costs—Annual 911 Reliability and Interoperability Certification. The Commission recently estimated that the existing 911 Reliability Certification filing requirement imposes a total cost for all CSPs of $14,446,785 annually.[276] This figure estimates 168,651 total burden hours across all CSPs at appropriate labor costs,[277] for an average compliance cost of $48,156 for each of 300 estimated annual filers. We anticipate these costs will be reduced consistent with the reduction in total filing entities to approximately 100 as the NG911 transition progresses. Using the average cost of $48,156 and multiplying by 100, that would result in a total annual estimated cost for all CSPs of $4,815,600. However, those figures represent the costs of an existing requirement adopted in 2013. We therefore further estimate that the incremental costs from today's proposals further specifying the NG911 equivalent facilities, functional equivalents, and best practice benchmarks of CSPs will be minimal, which we conservatively estimate at a 10% increase, or $481,560 per year. We seek comment on this estimate. We also seek comment on whether our proposals to move to drop-down reporting, and to allow certification to NG911 IP-specific benchmarks instead of requesting alternative measures reports for those practices, will further reduce reporting burdens.

Comparison of Costs and Benefits. Based on the foregoing, we conservatively estimate the benefits of today's proposals at approximately $304 million annually,[278] and the maximum

SIP. An Audiocodes Mediant 500 gateway, for example, costs approximately $1000, and a Mediant 1000, which has much more capability than a smaller carrier requires is approximately $5000.'').

[268] *See* ''Industrial Networking Solutions,'' UPS cost quote of $3,075 at 75 *https://www.industrialnetworking.com/Manufacturers/APC-Tower-Uninterruptible-Power-Supplies-UPS/APC-Smart-UPS-X-Uninterruptible-power-supply-SMX3000RMLV2UNC* (last visited Feb. 14, 2025).

[269] *See* ''QuoteColo,'' server collocation quote at *https://www.quotecolo.com/rack-space-rental/* ($700 per month for ''Full rack space—appropriate for medium and large web based companies seeking a primary and/or disaster recovery rack space data center.'') (last visited Feb. 14, 2025).

[270] We calculate total one-time costs as follows: ($5,000 server cost + $3,000 UPS device) × 25 entities = $200,000. The collocation cost is calculated as: $700/month × 12 months × 25 entities = $210,000 per year.

[271] *See* ''Enterprise Networking Planet,'' IP network monitoring pricing of approximately $2,000 per year at *https://www.enterprisenetworkingplanet.com/guides/network-monitoring-tools/* (last visited Feb. 14, 2025).

[272] The mean hourly wage for software developers in the telecommunications industry in May 2023 is $63.75. See Bureau of Labor Statistics, *May 2023 National Industry-Specific Occupational Employment and Wage Estimates NAICS 517000—Telecommunications, https://www.bls.gov/oes/current/naics4_517000.htm* (*BLS Telecommunications Wages*) (*see* Occupation Code 15–1252 ''Software Developers'').

[273] We markup wages for software developers by 45% to account for benefits. According to the Bureau of Labor Statistics, as of June 2024, civilian wages and salaries across all sectors averaged $31.80/hour and benefits averaged $14.41/hour. Total compensation therefore averaged $31.80 + $14.41, rounded to $46.21. *See* Press Release, Bureau of Labor Statistics, *Employer Costs for Employee Compensation—June 2024* (Sept. 10, 2024), *https://www.bls.gov/news.release/pdf/ecec.pdf.* Using these figures, benefits constitute a markup of $14.41/$31.80 ~ 45% (*Compensation Benefit Mark-up*).

[274] The mean hourly wage for computer network architects in the telecommunications industry in May 2023 is $54.95. *BLS Telecommunications Wages* (*see* Occupation Code 15–1241 ''Computer Network Architects''). The Bureau of Labor Statistics considers the title ''computer network architect'' to be synonymous with ''network engineer.'' Bureau of Labor Statistics, *Computer Network Architects: What Computer Network Architects Do, https://www.bls.gov/ooh/computer-and-information-technology/computer-network-architects.htm#tab-2* (visited Feb. 15, 2025).

[275] The mean hourly wage for telecommunications equipment installers and repairers in the telecommunications industry in May 2023 is $32.26. *BLS Telecommunications Wages* (*see* Occupation Code 49–2022 ''Telecommunications Equipment Installers and Repairers, Except Line Installers''). We mark up wages for telecommunications equipment installers and repairers by 45% to account for benefits. $32.26 × 1.45 = $46.78.

[276] *See Improving 911 Reliability,* OMB Control No. 3060–1202, Supporting Statement at 10 (Oct. 10, 2023), *https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202309-3060-007* (*October 2023 OMB Submission*).

[277] For certification labor cost estimates used in the *October 2023 OMB Submission,* we used the job categories of ''Miscellaneous Media and Communication Worker,'' ''Chief Executive,'' and ''Electronic Engineer, Except Computer'' and their respective mean hourly wages. *See* Bureau of Labor Statistics, Economic News Release, National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2022 (May 2022) *https://www.bls.gov/news.release/ocwage.t01.htm.* For miscellaneous communications worker, we began with the mean hourly wage $36.94 and multiplied by 1.5 to account for benefits to $55.41, then rounded down to $55. For chief executive, we used the mean hourly wage of $118.48, multiplied by 1.5 to account for benefits, and rounded up. $118.48 × 1.5 = $177.72, rounded to $178/hour. For electronic engineer, we used the mean hourly wage of $56.95, multiplied by 1.5 to account for benefits, and rounded down. $56.95 × 1.5 = $85.425, rounded to $85/hour.

[278] The mortality reduction benefit per fatality in 2023 is estimated at $13.2 million by the U.S. Department of Transportation, *Departmental Guidance on Valuation of a Statistical Life in*

Continued

worst-case costs at approximately $2.5 million in one-time expenses [279] and $6.7 million in annual recurring costs.[280] The benefits therefore outweigh the costs. We seek comment on this conclusion.

G. Pursuing a Deregulatory Agenda

As discussed above, today we propose to eliminate, consolidate, or streamline existing regulations contained in Part 9, Subpart H of our regulations.[281] Specifically, today we propose the following regulatory reductions. Current reliability rules 9.19(c)(1) to (3) contain 25 subparts and 876 words. Today's proposed amendments reduce rules 9.19(c)(1) to (3) to 9 subparts and 574 words. In addition, we propose that the recordkeeping requirements at rule 9.19(d)(3), which currently contain three subparts and total 251 words, be reduced to a single section containing 102 words. We also propose to substantially reduce the complexity and time-burdens of filing annual reliability certifications by streamlining and simplifying our CSP reporting obligations. These regulatory reductions are described further above in this FNPRM, the anticipated cost savings of these reductions are described above, and the rules reductions are shown below in the proposed rules. We tentatively conclude that these regulatory reductions will make our rules easier ''for the average person or business to understand,'' reduce compliance costs, and ''reduce the risk of costs of non-compliance.'' [282] We seek comment on any additional 911 reliability rules at Part 9, Subpart H and related certification filing compliance burdens that should be eliminated, consolidated, or streamlined consistent with the public interest.

Procedural Matters

Regulatory Flexibility Act. The Regulatory Flexibility Act of 1980, as amended (RFA),[283] 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.'' [284] Accordingly, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning potential rule and policy changes contained in this FNPRM. The IRFA is set forth in Appendix B. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

Paperwork Reduction Act. This FNPRM may contain proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on any information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, we seek specific comment on how we might ''further reduce the information collection burden for small business concerns with fewer than 25 employees.'' [285]

Initial Regulatory Flexibility Analysis

As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Further Notice of Proposed Rulemaking (FNPRM). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines in the FNPRM. The Commission will send a copy of the FNPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the FNPRM and IRFA (or summaries thereof) will be published in the **Federal Register**.

A. Need for, and Objectives of, the Proposed Rules

In the FNPRM, the Commission takes steps to improve the reliability and interoperability of Next Generation 911 (NG911) networks nationwide to ensure the American public can continue to reach emergency services without undue delay or disruption. Following the devastating impact of the June 2012 ''derecho'' storm to 911 services, the Commission determined that reliability, resiliency, and availability of 911 services could be improved through implementation of network-reliability best practices and other sound engineering principles, and accordingly adopted 911 reliability certification rules in 2013 applicable to certain entities providing 911 services to Public Safety Answering Points (PSAPs). These entities were designated as ''covered 911 service providers'' (CSPs). Since 2013, the Commission has taken steps to facilitate the transition from legacy 911 to NG911. Most recently, the Commission adopted a Report and Order to facilitate an orderly and coordinated transition from legacy 911 systems to NG911 systems for 911 Authorities and originating service providers (OSPs). The proposals in the FNPRM aim to ensure that NG911 is fully accessible to all Americans which requires that among other things NG911 networks have the capacity to handle multimedia NG911 calls from users including those with disabilities that include the transmission of texts, photos, videos, and data, and that NG911 networks have the requisite reliability and interoperability to seamlessly transfer 911 calls and data.

The NG911 transition represents a significant change in the 911 network architecture which will substantially alter the class of entities that are providing critical 911 services, requiring an update to which entities are 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 by a variety of service providers, including Emergency

Economic Analysis (May 7, 2024), *https://www.transportation.gov/office-policy/transportation-policy/revised-departmental-guidance-on-valuation-of-a-statistical-life-in-economic-analysis*). 23 estimated lives saved per year times $13.2 million is approximately $304 million per year.

[279] Total one-time costs include $1 million in router costs, $200,000 in server and UPS costs, $200,000 in IP network monitoring one-time cost, $200,000 in interoperability one-time cost and $875,568 in software, engineering, and installation labor costs = $2,475,568, rounded up to $2.5 million.

[280] Annual costs of $6.7 million include $3 million in transport path diversity costs, $2.4 million in incremental cost of the critical circuit auditing and tagging per year, $210,000 in annual collocation costs, $260,000 in annual IP network monitoring cost, $260,000 in annual interoperability cost, and $481,560 in incremental annual reporting costs, summed to $6,611,560 and rounded up to $6.7 million.

[281] *See Unleashing Prosperity Through Deregulation,* Executive Order (Jan. 31, 2025), *https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-prosperity-through-deregulation/*.

[282] *Id.*

[283] 5 U.S.C. 603. The RFA, 5 U.S.C. 601–612, was amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Public Law 104–121, Title II, 110 Stat. 857 (1996).

[284] 5 U.S.C. 605(b).

[285] 44 U.S.C. 3506(c)(4).

Services IP Network (ESInet) operators, Next Generation Core Services (NGCS) providers, and various third-party platforms providing services to OSPs. As the NG911 transition progresses, many smaller RLECs who are currently CSPs 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.

The Commission estimates that this new group of NG911 CSPs will be mostly larger national or regional providers, and they will provide most of the specialized critical bottleneck facilities in the NG911 environment, including ''Location Information Servers (LIS) as a service'' provided to OSPs, major transport facilities, VoIP Positioning Centers or traffic aggregation facilities, and LNG facilities at the NG911 Delivery Point. We anticipate these larger entities will provide critical 911 facilities and services on a contract and for-hire basis to the larger group of approximately 2,200 OSPs offering 911 call origination service to the public. We further anticipate that, over the estimated five years of the NG911 transition, the overall number of CSPs will shrink, leaving mostly a different group of entities as the critical bottleneck facilities providers in the NG911 ecosystem. Multiple RLECs that were CSPs have already notified the Commission's public Safety and Homeland Security Bureau (Bureau) that they have ceased providing the services of a CSP.

The FNPRM proposes rules intended to account for these developments in the NG911 transition, and to ensure the reliability and interoperability of NG911 as the technological and regulatory landscape evolves. In particular, the FNPRM proposes to revise the Commission's 911 reliability rules to ensure their continued effectiveness for NG911 systems. The rules adopted in 2013 codified in § 9.19 require CSPs to certify annually that they have ''take[n] reasonable measures to provide reliable 911 service with respect to circuit diversity, central-office backup power, and diverse network monitoring.'' The FNPRM proposes to update the Commission's reliability rules in § 9.19 as described below.

The Commission proposes to update the definition of ''covered 911 service provider'' or CSP in § 9.19(a) of the Commission's existing 911 reliability rules to specify how the rules apply to service providers that control or operate critical pathways and components of NG911 ecosystem networks. The current CSP definition focuses on providers of certain network facilities and capabilities directly serving PSAPs using descriptions specific to legacy 911 systems, but also states that the rules apply to the ''functional equivalents'' or ''equivalent facilities'' in the NG911 environment. We propose to specify which critical NG911 ecosystem facilities and capabilities are among the functional equivalents referred to in the current rule, and that providers of these capabilities therefore fall within the definition of CSPs.

We also propose to expand the CSP definition to apply to additional providers of critical connectivity in the NG911 environment, whether they directly serve PSAPs or not. These new proposed CSP entities are: (1) operators of LISs or equivalent IP 911 location databases; (2) operators of Legacy Network Gateways (LNGs); (3) operators of Major Transport Facilities that exceed Optical Carrier 3 (OC3) capacity and carry 911 traffic from multiple OSPs for ultimate delivery to NG911 Delivery Points or Emergency Services IP Networks (ESInets); (4) operators of IP Traffic Aggregation Facilities that carry 911 traffic from multiple OSPs towards ultimate transmission to an NG911 Delivery Point or ESInet; and (5) operators of interstate interconnecting facilities between ESInets. We also update § 9.19(a) to include defined terms consistent with the proposed rules we discuss in the FNPRM.

In § 9.19(c) the Commission proposes to update the reasonable reliability standards that providers of critical NG911 ecosystem functions must employ to ensure the reliable delivery of 911 traffic to NG911 delivery points. We believe such action is needed to ensure the reliability of critical transport, aggregation, and data facilities in NG911 networks at the interstate and national level and the accessibility of NG911 services.

In § 9.19(c)(4) the Commission proposes updates to establish NG911 interoperability requirements for interstate transfer of 911 traffic between ESInets to optimize PSAP call transfer capabilities during service disruptions. We seek to ensure that PSAPs can transfer calls to nearby PSAPs located across state borders with minimal need for the traffic to be retranslated or reformatted in order for such transfers to occur. We further propose to harmonize this action with our current 911 reliability certification rules in § 9.19(c) by adding an interoperability certification to the rules. We also seek updated information on interstate interoperability by type of service, with particular emphasis on services used by consumers, including those with accessibility needs.

In § 9.19(d) the Commission proposes updates to modify the certification and oversight mechanisms in our 911 reliability rules to improve implementation of reliability and interoperability in NG911 systems. We propose expansion of the ''Confidential Treatment'' provisions to enable state and local 911 Authorities to obtain reliability and interoperability certifications directly from CSPs, so that 911 Authorities can more easily exercise their existing authority to address reliability, interoperability, and accessibility needs within their jurisdictions. We also propose to modify § 9.19(d) to include the compliance schedule for the NG911 reliability and interoperability phase-in in the FNPRM.

The Commission also proposes to add a new § 9.19(e) to provide guidance on the Bureau's procedures for remediation investigations and handling reports from 911 Authorities regarding reliability and interoperability concerns. In addition, we seek comment on adding a new § 9.19(f) to create a petition process for 911 Authorities to submit allegations of violations of our 911 reliability and interoperability rules to the Bureau.

Finally, the Commission believes that the proposals we discuss in the FNPRM and summarize above 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. Legal Basis

The proposed action is authorized pursuant to sections 1, 2, 4(i), 201, 214, 222, 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, 222, 225, 251(e), 301, 303, 316, 332; the Wireless Communications and Public Safety Act of 1999, Public Law 106–81, 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, Public Law 111–260, 47 U.S.C. 615c.

C. Description and Estimate of the Number of Small Entities to Which the Proposed 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 proposed rules, if adopted. 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.

Small Businesses, Small Organizations, Small Governmental Jurisdictions. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, 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, the type of small entity described as a ''small organization'' is generally ''any not-for-profit enterprise which is independently owned and operated and is not dominant in its field.'' The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide, for tax year 2022, there were approximately 530,109 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

Finally, the small entity described as a ''small governmental jurisdiction'' is defined generally as ''governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand.'' U.S. Census Bureau data from the 2022 Census of Governments indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,845 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts) with enrollment populations of less than 50,000. Accordingly, based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 entities fall into the category of ''small governmental jurisdictions.''

Advanced Wireless Services (AWS)—(1,710–1,755 MHz and 2,110–2,155 MHz bands (AWS–1); 1,915–1,920 MHz, 1,995–2,000 MHz, 2,020–2,025 MHz and 2,175–2,180 MHz bands (AWS–2); 2,155–2,175 MHz band (AWS–3); 2,000–2,020 MHz and 2,180–2,200 MHz (AWS–4)). Spectrum is made available and licensed in these bands for the provision of various wireless communications services. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to these services. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus, under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

According to Commission data as of December 2021, there were approximately 4,472 active AWS licenses. The Commission's small business size standards with respect to AWS involve eligibility for bidding credits and installment payments in the auction of licenses for these services. For the auction of AWS licenses, the Commission defined a ''small business'' as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a ''very small business'' as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. Pursuant to these definitions, 57 winning bidders claiming status as small or very small businesses won 215 of 1,087 licenses. In the most recent auction of AWS licenses 15 of 37 bidders qualifying for status as small or very small businesses won licenses.

In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

All Other Telecommunications. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Providers of internet services (*e.g.,* dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of ''All Other Telecommunications'' firms can be considered small.

Broadband Personal Communications Service. The broadband personal communications services (PCS) spectrum encompasses services in the 1,850–1,910 and 1,930–1,990 MHz bands. The closest industry with a SBA small business size standard applicable to these services is Wireless Telecommunications Carriers (except Satellite). The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

Based on Commission data as of November 2021, there were approximately 5,060 active licenses in the Broadband PCS service. The Commission's small business size standards with respect to Broadband PCS involve eligibility for bidding credits and installment payments in the auction of licenses for these services. In auctions for these licenses, the Commission defined ''small business'' as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $40 million for the preceding three

years, and a ''very small business'' as an entity that, together with its affiliates and controlling interests, has had average annual gross revenues not exceeding $15 million for the preceding three years. Winning bidders claiming small business credits won Broadband PCS licenses in C, D, E, and F Blocks.

In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

Cable System Operators (Telecom Act Standard). The Communications Act of 1934, as amended, contains a size standard for a ''small cable operator,'' which is ''a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000.'' For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 498,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator. Based on industry data, only six cable system operators have more than 498,000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

Competitive Local Exchange Carriers (CLECs). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local service providers. Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Incumbent Local Exchange Carriers (Incumbent LECs). Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers. Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

Interexchange Carriers (IXCs). Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

Local Exchange Carriers (LECs). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were fixed local exchange service providers. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Lower 700 MHz Band Licenses. The lower 700 MHz band encompasses spectrum in the 698–746 MHz frequency bands. Permissible operations in these bands include flexible fixed, mobile, and broadcast uses, including mobile and other digital new broadcast operation; fixed and mobile wireless commercial services (including FDD and TDD-based services); as well as fixed and mobile wireless uses for private, internal radio needs, two-way interactive, cellular, and mobile television broadcasting services. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to licenses providing services in these bands. The SBA small business

size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

According to Commission data as of December 2021, there were approximately 2,824 active Lower 700 MHz Band licenses. The Commission's small business size standards with respect to Lower 700 MHz Band licensees involve eligibility for bidding credits and installment payments in the auction of licenses. For auctions of Lower 700 MHz Band licenses the Commission adopted criteria for three groups of small businesses. A very small business was defined as an entity that, together with its affiliates and controlling interests, has average annual gross revenues not exceeding $15 million for the preceding three years, a small business was defined as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $40 million for the preceding three years, and an entrepreneur was defined as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $3 million for the preceding three years. In auctions for Lower 700 MHz Band licenses seventy-two winning bidders claiming a small business classification won 329 licenses, twenty-six winning bidders claiming a small business classification won 214 licenses, and three winning bidders claiming a small business classification won all five auctioned licenses.

In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

Offshore Radiotelephone Service. This service operates on several UHF television broadcast channels that are not used for television broadcasting in the coastal areas of states bordering the Gulf of America,[286] and is governed by subpart I of Part 22 of the Commission's Rules. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to this service. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus, under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small. Additionally, based on Commission data, as of December 2021, there was one licensee with an active license in this service. However, since the Commission does not collect data on the number of employees for this service, at this time we are not able to estimate the number of licensees that would qualify as small under the SBA's small business size standard.

Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment. Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment. The SBA small business size standard for this industry classifies businesses having 1,250 employees or less as small. U.S. Census Bureau data for 2017 show that there were 656 firms in this industry that operated for the entire year. Of this number, 624 firms had fewer than 250 employees. Thus, under the SBA size standard, the majority of firms in this industry can be considered small.

Rural Radiotelephone Service. Neither the Commission nor the SBA have developed a small business size standard specifically for small businesses providing Rural Radiotelephone Service. Rural Radiotelephone Service is radio service in which licensees are authorized to offer and provide radio telecommunication services for hire to subscribers in areas where it is not feasible to provide communication services by wire or other means. A significant subset of the Rural Radiotelephone Service is the Basic Exchange Telephone Radio System (BETRS). Wireless Telecommunications Carriers (*except* Satellite), is the closest applicable industry with a SBA small business size standard. The SBA small business size standard for Wireless Telecommunications Carriers (*except* Satellite) classifies firms having 1,500 or fewer employees as small. For this industry, U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated for the entire year. Of this total, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that the majority of Rural Radiotelephone Services firm are small entities. Based on Commission data as of December 27, 2021, there were approximately 119 active licenses in the Rural Radiotelephone Service. The Commission does not collect employment data from these entities holding these licenses and therefore we cannot estimate how many of these entities meet the SBA small business size standard.

Satellite Telecommunications. This industry comprises firms ''primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications.'' Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $44 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year. Of this number, 242 firms had revenue of less than $25 million. Consequently, using the SBA's small business size standard most satellite telecommunications service providers can be considered small entities. The Commission notes however, that the SBA's revenue small business size standard is applicable to a broad scope of satellite telecommunications providers included in the U.S. Census Bureau's Satellite Telecommunications industry definition. Additionally, the Commission neither requests nor collects annual revenue information from satellite telecommunications providers, and is therefore unable to more accurately estimate the number of

[286] Exec. Order No. 14172, 90 FR 8630, 2025 WL 343885 (Jan. 20, 2025). The Gulf of America, formerly known as the Gulf of Mexico.

satellite telecommunications providers that would be classified as a small business under the SBA size standard.

Semiconductor and Related Device Manufacturing. This industry comprises establishments primarily engaged in manufacturing semiconductors and related solid state devices. Examples of products made by these establishments are integrated circuits, memory chips, microprocessors, diodes, transistors, solar cells and other optoelectronic devices. The SBA small business size standard for this industry classifies entities having 1,250 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 729 firms in this industry that operated for the entire year. Of this total, 673 firms operated with fewer than 250 employees. Thus under the SBA size standard, the majority of firms in this industry can be considered small.

Telecommunications Relay Service (TRS) Providers. Telecommunications relay services enable individuals who are deaf, hard of hearing, deafblind, or who have a speech disability to communicate by telephone in a manner that is functionally equivalent to using voice communication services. Internet-based TRS connects an individual with a hearing or a speech disability to a TRS communications assistant using an internet Protocol-enabled device via the internet, rather than the public switched telephone network. Video Relay Service (VRS) one form of internet-based TRS, enables people with hearing or speech disabilities who use sign language to communicate with voice telephone users over a broadband connection using a video communication device. Internet Protocol Captioned Telephone Service (IP CTS) another form of internet-based TRS, permits a person with hearing loss to have a telephone conversation while reading captions of what the other party is saying on an internet-connected device. A third form of internet-based TRS, internet Protocol Relay Service (IP Relay), permits an individual with a hearing or a speech disability to communicate in text using an internet Protocol-enabled device via the internet, rather than using a text telephone (TTY) and the public switched telephone network. Providers must be certified by the Commission to provide VRS and IP CTS and to receive compensation from the TRS Fund for TRS provided in accordance with applicable rules. Analog forms of TRS, text telephone (TTY), Speech-to-Speech Relay Service, and Captioned Telephone Service, are provided through state TRS programs, which also must be certified by the Commission.

Neither the Commission nor the SBA have developed a small business size standard specifically for TRS Providers. All Other Telecommunications is the closest industry with a SBA small business size standard. Internet Service Providers (ISPs) and Voice over internet Protocol (VoIP) services, via client-supplied telecommunications connections are included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on Commission data there are 14 certified internet-based TRS providers and two analog forms of TRS providers. The Commission however does not compile financial information for these providers. Nevertheless, based on available information, the Commission estimates that most providers in this industry are small entities.

Upper 700 MHz Band Licenses. The upper 700 MHz band encompasses spectrum in the 746–806 MHz bands. Upper 700 MHz D Block licenses are nationwide licenses associated with the 758–763 MHz and 788–793 MHz bands. Permissible operations in these bands include flexible fixed, mobile, and broadcast uses, including mobile and other digital new broadcast operation; fixed and mobile wireless commercial services (including FDD- and TDD-based services); as well as fixed and mobile wireless uses for private, internal radio needs, two-way interactive, cellular, and mobile television broadcasting services. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to licenses providing services in these bands. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Thus, under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

According to Commission data as of December 2021, there were approximately 152 active Upper 700 MHz Band licenses. The Commission's small business size standards with respect to Upper 700 MHz Band licensees involve eligibility for bidding credits and installment payments in the auction of licenses. For the auction of these licenses, the Commission defined a ''small business'' as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years, and a ''very small business'' an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. Pursuant to these definitions, three winning bidders claiming very small business status won five of the twelve available licenses.

In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

Wired Telecommunications Carriers. The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964

firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Wireless Communications Services. Wireless Communications Services (WCS) can be used for a variety of fixed, mobile, radiolocation, and digital audio broadcasting satellite services. Wireless spectrum is made available and licensed for the provision of wireless communications services in several frequency bands subject to Part 27 of the Commission's rules. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with an SBA small business size standard applicable to these services. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

The Commission's small business size standards with respect to WCS involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in WCS. When bidding credits are adopted for the auction of licenses in WCS frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in the designated entities section in Part 27 of the Commission's rules for the specific WCS frequency bands.

In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

Wireless Telecommunications Carriers (except Satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Wireless Telephony. Wireless telephony includes cellular, personal communications services, and specialized mobile radio telephony carriers. The closest applicable industry with an SBA small business size standard is Wireless Telecommunications Carriers (except Satellite). The size standard for this industry under SBA rules is that a business is small if it has 1,500 or fewer employees. For this industry, U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 331 providers that reported they were engaged in the provision of cellular, personal communications services, and specialized mobile radio services. Of these providers, the Commission estimates that 255 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

The FNPRM proposes and seeks comment on revisions to requirements that may affect the reporting, recordkeeping, and/or other compliance requirements for small and other entities that provide 911 services. As explained previously in this IRFA, the Commission anticipates the NG911 transition, and the conforming proposals in today's FNPRM will eliminate the burdens on most small entities currently subject to the 911 reliability rules since most small entities currently designated as CSPs will likely cease providing the services of a CSP. Therefore, the Commission also anticipates the proposals in the FNPRM will not continue to subject these small entities to the CSP regulations, and will not impose compliance obligations that require small entities to hire professionals. We expect the new requirements proposed in the FNPRM will generally apply to larger entities. Nevertheless, we summarize these requirements here.

In the FNPRM, the Commission proposes to maintain the current structure of the existing reliability regulations, which require all 911 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 an annual certification filing. The new compliance measures we proposed in the FNPRM update best practice benchmarks applicable to NG911 facilities, add a ''reasonable interoperability'' requirement and best practice benchmarks for certain CSPs, and modify the certification reporting process for CSPs.

The Commission tentatively estimates that the proposed reasonable reliability and interoperability requirements would affect approximately twenty-five NG911 providers imposing costs they are not already incurring. We further estimate the new certification reporting requirements will result in incremental compliance costs for approximately one-hundred NG911 providers. In the FNPRM, we seek comment on these estimates, and provide a breakdown of the estimated costs below for the relevant groups of NG911 providers.

NG911 Reliability Best Practices. The Commission anticipates that some entities will choose to satisfy the ''reasonable reliability'' requirement by meeting the three best practice

benchmarks to demonstrate presumptive reasonability. The first benchmark is physical diversity of network paths and circuits, to eliminate single points of failure in the call chain. For NG911 facilities, we propose that ''physical diversity'' would mean that critical paths established by CSPs must be geographically diverse, load-balanced, and capable of automatic failover to the backup element (*e.g.,* redundant routers or node connections and links) and automatic reroutes to redundant paths in the transport layer in the event of path failure. Redundant routers or node paths and links should be located in different geographic locations (*i.e.,* in different physical facilities). We propose that this benchmark would apply to Major Transport Providers and IP Aggregation Facilities. The Commission estimates that all entities choosing to meet the physical diversity benchmark will incur approximately $1 million in redundant router costs, and $3 million annually in short and long distance transport costs for the 25 estimated affected CSPs.

The second benchmark is operational integrity. For NG911 facilities, the operational integrity benchmark means maintaining redundant and geographically distributed backups located in different facilities sufficient to ensure that a failure of any localized facility will not interrupt 911 traffic, and having appropriate continuous power, such as an uninterruptible power supply (UPS) device. In 2014, the Commission observed that network architectures using ''two active databases in different geographic locations, each of which is capable of handling all 911 call traffic in the event of a fault in the other database, will be more reliable and resilient than those that route all calls through a single active database with backup equipment on passive 'standby' mode.'' We propose this benchmark would apply to LIS and LNG facilities used in NG911 ecosystems.

Relying on data in the NG911 proceeding, the Commission conservatively estimates the cost of diverse LNG or LIS servers at approximately $5,000 each. We further estimate the cost of uninterruptible power supply or UPS devices on the high-end of approximately $3,000 per unit. Finally, we conservatively estimate the cost of any needed diverse secondary server collocation ''full rack'' space at approximately $700 per month. This amounts to $200,000 in one-time costs, and recurring cost of $210,000 annually for the estimated 25 CSPs that will be affected.

The third benchmark is network monitoring. The Commission proposes to specify NG911 monitoring technologies identified in prior Commission orders as methods of compliance. Specifically, we propose NG911-appropriate standards for network monitoring relying on automatic disruption detection and alarms. We propose this monitoring benchmark would apply to path diversity facilities of Major Transport Providers and IP Aggregation Facilities such as routers, nodes, and node links, as well as to LNG and LIS facilities used in NG911 ecosystems. The Commission estimates the costs of IP network monitoring capability as similar in facilities as those of operational integrity for LIS and LNG. Thus, our cost estimate starts with $200,000 in one-time costs, and $210,000 annually similar to LIS and LNG, and we add an additional estimated $50,000, for $2,000 per year in monitoring software licensing costs, which we multiply by the 25 estimated affected CSPs for a total cost of $260,000 annually.

NG911 Reasonable Interoperability and Best Practices. The Commission proposes to adopt interstate interoperability reasonableness requirement for entities operating ESInet interstate interconnecting facilities. We also propose to apply the existing annual certification requirement for interoperability to these new CSPs. In the annual certification our proposed requirement would require CSPs operating interstate ESInet interconnecting facilities to certify whether their facilities achieve interoperability for exchanged 911 traffic sufficiently to enable complete interstate transfers between ESInets. To demonstrate presumptive reasonableness, we propose that CSPs annually certify that their interstate interconnecting ESInet facilities have deployed conformance-tested equipment as well as annually certify that it has tested its interstate interoperability capabilities. If a CSP does not conform to the benchmark elements, the CSP would be required to certify to its alternative measures used, as the current rules require all CSPs to do for reliability. The Commission tentatively estimates the costs of acquiring interoperability capability as substantially similar to those of IP network monitoring. Accordingly, we tentatively estimate $200,000 in one-time costs and $260,000 annually as the cost of compliance of this proposal.

Technical Labor Costs for Compliance. The Commission estimates that there will be additional labor costs for programming, engineering, and installation for integrating and/or testing each of the above reliable and interoperable facilities. First, we assume the average wage of a software developer is $63.75/hour, with a 45% markup for benefits, to arrive at $92.44/hour as the compensation rate for software developers. Next, we assume the average wage of computer network engineers is $54.95/hour, with a 45% markup for benefits, to arrive at $79.68/hour as the compensation rate for network engineers. We also assume the average benefits-adjusted wage for telecommunications equipment installers and repairers is $46.78 per hour. For additional labor costs of meeting benchmarks not already implemented we tentatively estimate approximately 160 labor-hours total in each of those three categories. We therefore calculate an estimated labor cost of approximately $14,790 for software labor, $12,748 for engineering labor, and $7,484 for installation labor, for a total cost of $35,023 per CSP. Applying this cost estimate to the 25 CSPs that will begin meeting the reasonableness benchmarks for the first time as a result of today's proposed rules, the total estimated one-time labor cost is $875,568.

911 Reliability and Interoperability Annual Certification. In the FNPRM, the Commission proposes that all NG911 CSPs must file an annual 911 reliability and interoperability certification indicating whether they meet the best practice benchmarks or are using alternative measures to achieve reasonable reliability or interoperability. This is an expansion of the existing annual 911 reliability requirement. In the next section of this IRFA we discuss the measures and revisions we propose in the FNPRM to streamline the certification form and reporting process to minimize burdens for affected entities.

The Commission recently estimated that the existing 911 Reliability Certification filing requirement imposes a total cost for all CSPs of $14,446,785 annually. This cost estimates 168,651 total burden hours across all CSPs at appropriate labor costs, for an average compliance cost of $48,156 for each of 300 estimated annual filers. As the NG911 transition progresses, the Commission anticipates these costs will decrease consistent with the reduction in the total number of filing entities. We estimate the filing entities will decrease from 300 to approximately 100 filing entities. Using the average cost of $48,156 per CSP and multiplying by 100, would result in a total annual estimated cost for all CSPs of $4,815,600. These costs however

represent the costs of compliance with the existing requirements the Commission adopted in 2013. To account for the incremental costs for the proposals in the FNPRM further specifying the NG911 equivalent facilities, functional equivalents, and best practice benchmarks of CSPs which will be minimal, we conservatively estimate a 10% increase. The incremental cost of a 10% increase results in $481,560 per year.

Record Retention and Compliance Timeframe. The proposed rules in the FNPRM include revision of the existing record retention requirement in § 9.19(d)(3) to include a requirement for CSPs to retain 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, to support the Annual 911 reliability and interoperability certification. The FNPRM also proposes codification of the compliance timeframe for the NG911 reliability and interoperability phase-in which grants CSPs that would be subject to the proposed requirements if adopted, one year after all of the information and recordkeeping requirements subject to approval by the Office of Management and Budget (OMB) have been approved to comply.

The Commission estimates that the maximum costs of the compliance and reporting obligations imposed on CSPs subject to the proposals in the FNPRM would be approximately $2.5 million in one-time expenses and $6.7 million in annual recurring costs. At the same time the Commission estimates that there will be a benefit of approximately $304 million annually for the estimated lives saved as a result of the proposals in the FNPRM.

E. Steps Taken To Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): ''(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for such small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.''

Some Alternatives Considered. To reduce the burdens for small entities, the Commission specifically considers and seeks comment on whether providing increased flexibility to providers or businesses classified by SBA's small business size standards as small could alleviate the burden of any reporting requirements. Further, the Commission considers, but declines to include all indirect service providers—which could include small entities, within the definition of CSPs to avoid imposing burdens of outage reporting and certification requirements on indirect providers of essential NG911 services. Instead we retain the direct service requirement amending § 9.19 to specify that CSPs directly serving PSAPs are responsible for ensuring the reliability of all of the NG911 capabilities they provide to the PSAP regardless of how the NG911 capabilities are provisioned. Coincident with the Commission's proposed expansion of the classes of entities covered by our NG911 reliability rules to include entities that perform critical NG911 functions, we also consider whether to amend the outage reporting requirements in § 4.5(e) to include the NG911 entities subject to our 911 reliability rules. Additionally, we explore whether there are measures in addition to the annual certification that can be taken to further promote 911 reliability and interoperability, such as implementing an outcome-based standard that establishes how many annual user minutes of 911 traffic could be interrupted by network or facility outages and still be considered reasonable, beneath which a CSP is subject to remediation orders, or adopting a similar interoperability standard based on the percentage of interstate 911 call transfers which fail completely, or fail to include caller location or other data.

Eliminating Compliance Burdens on Small Businesses. Today's FNPRM declines to extend the current reliability regulatory regime to continue to cover small entities—OSPs and RLECs who will be retiring from the provision of certain legacy 911 facilities during the NG911 transition. While all entities in the 911 call chain including small OSPs play critical roles in ensuring 911 traffic gets delivered to PSAPs, the Commission recognizes as some small entities indicate that the rules we propose in the FNPRM should only apply to ''bottleneck'' network facilities upon which multiple OSPs and PSAPs depend. Accordingly, we propose that smaller OSPs such as RLECs will no longer be subject to the reliability regulations or the annual certification filing requirement once they retire their legacy 911 routing, location, and trunking facilities and no longer provide direct services to PSAPs. This proposal should eliminate the economic burdens for the significant number of OSP and RLEC small entities that are currently subject to the reliability rules and to the annual certification filing requirement.

Cost Flexibility for Smaller Government Entities. As discussed above, the Commission tentatively proposes to keep the existing ''direct service to PSAPs'' condition for qualifying as a CSP for most entities that provide 911 routing, location services, and critical delivery paths to PSAPs. This preserves flexibility under our rules for portions of the NG911 networks on the state government and 911 Authority side of the NG911 cost allocation demarcation point. By keeping this condition, we ensure that 911 Authorities and state governments will have maximum flexibility in their service contracts with NG911 vendors, and the ability to make locally-appropriate decisions as to whether their vendors provide services directly to PSAPs or to another branch of government. This proposal ensures that 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.

Compliance Timelines. The compliance timeframe the Commission proposes in today's FNPRM provides CSPs subject to the requirements one year to comply after approval of all information and recordkeeping requirements subject to approval by the Office of Management and Budget (OMB). The one-year post OMB approval period would include the time needed for OMB to review and approve of a revised 911 reliability and interoperability certification form which we direct the PSHSB to implement. The Commission expects the burdens of compliance to be minimal since most of the benchmarks in the proposed rules already apply to covered entities providing NG911 equivalent services, which includes the reasonableness requirement which requires compliance

with either the alternative measures, or the current best practices. Thus, many CSPs that will be required to comply with the proposed rules are likely already in compliance. Further, the new benchmark practices we adopt are also standard IP network reliability measures that are generally being implemented for communications networks to meet expected quality of service standards. Therefore, the Commission believes this proposed compliance timeframe will give CSPs adequate notice and advance opportunity to prepare in accordance with ordinary business cycles, and at minimal cost.

Consolidations, Streamlining, and Simplifications of Compliance and Reporting Requirements. Today's FNPRM takes steps to ensure that all CSPs subject to the proposed reliability and interoperability rules can comply with the minimum necessary burden, reducing the compliance costs for regulated entities. For example, by specifying the NG911 best practice benchmarks in the regulations along with the legacy 911 benchmarks, CSPs will have greater certainty of what constitutes reasonable reliability and interoperability in the NG911 environment. Including these NG911 benchmarks in the regulations will further ease certification reporting burdens by allowing NG911 providers to certify they meet the benchmarks, rather than having to certify that they do not meet the legacy 911 benchmarks and then describe their alternative NG911 measures in narrative format for dozens or hundreds of facilities. Providing a description of alternative measures would be reserved for instances when there were deviations from the best practice benchmarks.

We also consider and propose to streamline the certification form by allowing CPSs to select alternative measures from a drop-down menu and then identify all facilities that use them, rather than the current process where CSPs list each facility and describe its alternative measure separately and narratively. We further propose to revise the certification form so that CSPs can select which facilities they operate from a drop-down menu, to reduce the burden of having to complete inapplicable portions of a form to answer ''not applicable'' and to provide a narrative explanation of why. Additionally, the FNPRM proposes to consolidate portions of rule 9.19 concerning alternative measures for reasonable reliability in order to reduce the complexity of complying with the certification form. The Commission specifically directs PSHSB to consider revisions to the certification form that, (1) allow CSPs to specify the type(s) of 911 facilities they are operating—legacy and/or NG91—in a way that constrains which best practice standard they are certifying to, (2) that will ensure NG911 CSPs do not have to submit narrative explanations of alternative measures for IP-based facilities if those facilities meet the regulatory best practice benchmarks for IP-based networks, and (3) that contain specified drop-down menu answers to replace the current free-form text reporting option for alternative measures or ''not applicable'' responses.

Finally, today's FNPRM proposes measures to minimize the burden on regulated entities subject the proposed requirements of § 9.19 by for example seeking to consolidate the paragraphs addressing alternative measures reporting in § 9.19(c)(1) to (3) to capture both legacy and NG911 providers. We also propose to consolidate and streamline the recordkeeping requirements in § 9.19(d)(3), to simplify compliance and better apply to all legacy 911 and NG911 CSPs.

F. Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rules

None.

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, Public Law 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, Public Law 111–260, 47 U.S.C. 615c, that this Further Notice of Proposed Rulemaking *is adopted.*

It is further ordered that the Commission's Office of the Secretary *shall send* a copy of this Further Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

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.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 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 reliability, interoperability, and redundancy 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 certifications filed in connection therewith, 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 a 911 reliability and interoperability certification pursuant to 47 CFR 9.19 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 certification.

* * * * *

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. The heading for subpart H is revised to read as follows:

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

■ 6. Amend § 9.19 by:
■ a. Revising the section heading;
■ b. Revising the heading of paragraph (a)(1);
■ c. Revising paragraphs (a)(2)(iv), and (a)(4)(i)(A) and (B);
■ d. Adding paragraphs (a)(4)(i)(C) through (G);
■ e. Revising paragraphs (a)(4)(ii)(A) and (B), (a)(5), (6), and (8);
■ f. Removing paragraphs (a)(9) and (10), and redesignating paragraph (a)(11) as paragraph (a)(9);
■ g. Adding paragraphs (a)(10) through (18);
■ h. Revising paragraphs (b), (c), and (d); and
■ i. Adding paragraphs (e) through (g).

The revisions and additions read as follows:

§ 9.19 Reliability and interoperability of covered 911 service providers.

(a) * * *

(1) *Monitoring aggregation point.*

* * *

(2) * * *

(iv) The term ''certification'' shall include the annual 911 reliability and interoperability certification under paragraph (c) of this section.

* * * * *

(4) * * *

(i) * * *

(A) Provides 911, E911, or NG911 (where ''NG911'' has the meaning given in § 9.28) capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities (including, but not limited to, NG911 Core Services (NGCS) Location Facilities or NGCS Routing Facilities), directly, by contract or tariffed service, whether via owned and operated facilities or leased or contracted facilities, to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as defined in § 9.3;

(B) Operates 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 (including NGCS Location Facilities or NGCS Routing Facilities), or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP;

(C) Operates a Location Information Server (LIS) as defined in § 9.28 or equivalent IP 911 location database;

(D) Operates a Legacy Network Gateway (LNG) used for conversion of Time Division Multiplexing (TDM) 911 traffic to Session Initiation Protocol (SIP) as defined in § 9.28;

(E) Operates a Major Transport Facility;

(F) Operates an IP Traffic Aggregation Facility; and/or

(G) Operates interstate interconnecting facilities between ESInets.

(ii) * * *

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

(B) Offers the capability to originate 911 calls, except to the extent the entity also operates the facilities or provides the services described in paragraph (a)(4)(i) of this section.

(5) *Critical 911 circuits and paths.* 911 facilities that either:

(i) Originate at a selective router or its functional equivalent (including facilities that collect or aggregate 911 traffic from multiple OSPs when performed at sites other than the central office hosting a selective router) and terminate in the central office that serves the PSAP(s) to which the selective router or its functional equivalent delivers 911 calls, including all equipment in the serving central office necessary for the delivery of 911 calls to the PSAP. Critical 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).

(ii) Transport 911 traffic via Major Transport Facilities to ultimate delivery at an NG911 Delivery Point or ESInet, including any intermediate paths in the chain of delivery.

(iii) Transport 911 traffic via IP Traffic Aggregation Facilities towards ultimate delivery at an NG911 Delivery Point or ESInet, 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 critical 911 circuits and paths are physically diverse.

* * * * *

(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 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 create physically diverse paths if routers are redundant, geographically diverse, load balanced, and each capable of automatic reroutes to more than one path in the event of failure.

* * * * *

(10) *Geographically distributed.* 911 network architecture is geographically distributed if 911 traffic can be delivered through more than one critical 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 Transport Facility.* Dedicated SIP transport facilities meeting or exceeding Optical Carrier 3 (OC3) in capacity that collect and/or transmit IP 911 traffic, either segregated or mixed with non-911 traffic, originated from multiple OSPs and transported over interstate routes, for ultimate transport and delivery to an NG911 Delivery Point or ESInet.

(13) *IP Traffic Aggregation Facility.* Facilities that collect and segregate IP 911 traffic from non-911 traffic for multiple OSPs, or transport such traffic for ultimate delivery to an NG911 Delivery Point or ESInet.

(14) *Operational integrity.* Network capability to ensure continuity of services via necessary continuous power and automated switchover to geographically diverse backup facilities

and configurations to prevent service disruption.

(15) *NGCS Location Facilities.* The Location Validation Function (LVF) and the Geographic Information System (GIS).

(16) *NGCS Routing Facilities.* The Emergency Call Routing Function (ECRF), Emergency Services Routing Proxy (ESRP), and the Policy Routing Function (PRF).

(17) *Interoperability standards testing.* Testing of a covered 911 service provider facilities that validates its NG911 interoperability solution conforms to a relevant commonly accepted standard in a way that increases the likelihood of interoperability.

(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 via their facilities.

(b) *Provision of reliable and interoperable 911 service.* All covered 911 service providers shall take reasonable measures to provide reliable and interoperable 911 service that ensures physical diversity, operational integrity, network monitoring, and interoperability for their covered 911 facilities. Performance of the elements of the certification set forth in paragraphs (c)(1) through (4) 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 in accordance with paragraph (c) of this section 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) *Annual 911 reliability and interoperability certification.* A certifying official of every covered 911 service provider shall submit an annual certification to the Commission. The certification shall address the following elements of reliability and interoperability:

(1) *Physical diversity.* (i) A covered 911 service provider shall certify that it has physical diversity for all critical 911 circuits and paths in its network. Physical diversity can be achieved for IP facilities by ensuring automatic rerouting capabilities, load balancing, and geographic distribution of routing facilities, transport nodes, and node links sufficient to eliminate all single points of failure; or for legacy facilities by conducting a diversity audit within the current calendar year and that all of the critical 911 circuits and paths in its network are tagged and are physically diverse such that no network or facility element constitutes a single point of failure.

(ii) If a covered 911 service provider does not conform with the applicable elements in paragraph (c)(1)(i) of this section, it must certify with respect to its non-conforming facilities: whether it has taken alternative measures to mitigate the risks of lack of physical diversity; whether it believes that the physical diversity requirement is not applicable to portions of its network; and to answer additional questions about the non-conforming portions of its network as directed by the Public Safety and Homeland Security Bureau (Bureau).

(2) *Operational integrity.* (i) 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; its LNG facilities; and/or its LIS facilities achieve operational integrity, which can be satisfied for IP facilities with automatic switchover capability to geographically diverse facilities and continuous power necessary to maintain operations; or with 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 necessary testing, equipment maintenance, generator design, and proper installation necessary to ensure the automatic and independent function of backup power generator facilities.

(ii) If a covered 911 service provider does not conform with the applicable elements in paragraph (c)(2)(i) of this section it must certify with respect to its non-conforming facilities: whether it has taken alternative measures to mitigate the risk of a loss of service; whether it believes that one or more of the requirements of paragraph (c)(2)(i) of this section are not applicable to its facilities; and to additional questions about the non-conforming facilities as directed by the Bureau.

(3) *Network monitoring.* (i) A covered 911 service provider shall certify whether it uses physically diverse monitoring systems to detect outages and disruptions in its covered 911 facilities. Physically diverse monitoring can be achieved for IP systems through the use of geographically distributed automatic disruption detection and alarm systems; or for legacy facilities, by maintaining and annually auditing physically diverse monitoring aggregation points, monitoring links, and NOCs.

(ii) If a covered 911 Service Provider does not conform with the applicable elements in paragraph (c)(3)(i) of this section, it must certify with respect to its non-conforming facilities: whether it has taken alternative measures to mitigate the risk of network monitoring failures; whether it believes that one or more of the requirements of paragraph (c)(3)(i) of this section are not applicable to its network; and to additional questions about the non-conforming facilities as directed by the Bureau.

(4) *Interoperability.* (i) A covered 911 service provider shall certify whether its interstate interconnecting ESInet facilities achieve interoperability for exchanged 911 traffic, as defined in section 9.28, sufficiently to enable complete transfers between ESInets. Interoperability can be achieved by conducting annual standards conformance testing and annual interoperability testing that validate the covered 911 service provider's interoperability for its interstate facilities.

(ii) If a covered 911 service provider does not conform with the applicable elements in paragraph (c)(4)(i) of this section, it must certify with respect to those facilities: whether it has taken alternative measures to ensure interoperability between ESInets in multiple states and providers to facilitate the exchange of 911 traffic, as defined in section 9.28; whether it believes that one or more of the requirements of paragraph (c)(4)(i) of this section are not applicable to its facilities; and to additional questions about the non-conforming facilities as directed by the Bureau.

(d) *Other matters*—(1) *NG911 reliability and interoperability phase-in.* Compliance for covered 911 service providers specified at paragraphs (a)(4)(i)(C) through (G) of this section that are not currently covered by paragraph (a)(4)(i)(A) or (B) will not be required until one year after Commission announcement in the **Federal Register** of approval of all information and recordkeeping requirements that may require review of the Office of Management and Budget, at which time this paragraph (d) will contain the compliance date.

(2) *Confidential treatment and 911 Authority access.* (i) The fact of filing or not filing an annual 911 reliability and interoperability certification and the responses on the face of such

certification forms shall not be treated as confidential.

(ii) Information submitted with such certifications 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 in or with respect to a certification.

(iii) 911 Authorities may request access to 911 reliability and interoperability certification data from the Chief of the Public Safety and Homeland Security Bureau, and such access shall be granted under the same terms and conditions as provided for access to NORS data under § 4.2 of this chapter. Notwithstanding other 911 reliability certifications data collection and reporting requirements in this section, covered 911 service providers must provide 911 reliability and interoperability certification information submitted to the Commission to 911 Authorities, as defined in § 9.28, upon request, except that they may omit or redact information relating to portions of their networks or facilities that are not located within and do not provide any service directly to the requesting 911 Authorities' jurisdiction. Covered 911 service providers must provide such information to 911 Authorities in the areas where they provide covered services or operate covered facilities, and the information must be provided no later than 14 days after a request. Covered 911 service providers may condition the granting of such requests on the 911 Authority executing a confidentiality agreement under terms not more restrictive than those set forth in § 4.2 of this chapter.

(3) *Record retention.* A covered 911 service provider shall retain records supporting the responses in a certification for two years from the date of such certification, 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 a certification hereunder 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.

(4) *Covered service cessation notices.* Covered 911 service providers that cease covered operations under this section must notify the FCC by filing a notification under penalty of perjury no later than 60 days after the cessation of service. Upon filing a notification with the Commission, covered 911 service providers must provide the same notifications to the 911 Authorities where their covered facilities are located and provide service to the 911 Authority.

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

(1) If certification filings or other information available to the Commission indicate that a covered 911 service provider's actions are deficient to demonstrate reasonable reliability or interoperability addressed in this subpart, the Bureau Chief may issue and electronically serve upon the covered 911 service provider a notice that describes any apparent deficiencies and proposes different or additional actions that the covered 911 service provider must take to mitigate the apparent deficiencies.

(2) A covered 911 service provider may submit a written response to a notice issued pursuant to paragraph (e)(1) of this section within 30 days of service of such notice. Service shall be made as directed by the Bureau.

(3) At any time after the 30th day following service of a notice issued pursuant to paragraph (e)(1) of this section, the Bureau Chief or other Bureau official acting on the Chief's delegated authority 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 to complete the required actions and may identify information that the provider must submit to demonstrate its compliance with the order.

(4) In addition to the procedures in paragraphs (e)(1) through (3) of this section, a 911 Authority may make referrals of concerns with covered 911 service providers' use of alternative measures or claims of inapplicability in the certification, or failure to accurately certify, or other reliability or interoperability concerns in the 911 Authority's jurisdiction to the Bureau Chief, for the Bureau Chief's evaluation, investigation, and other action at the Bureau Chief's discretion.

(f) *Petition process.* A 911 Authority may file a petition with the Bureau against a covered 911 service provider in its jurisdiction for using insufficient alternative measures or claiming inapplicability in its certification, or failure to accurately certify, or for other lack of reasonable network practices in conformity with paragraph (b) of this section. In such proceedings, the covered 911 service provider will have the burden of demonstrating that its covered facilities and network practices are reasonable, unless it has demonstrated presumptive reasonability by affirmatively certifying it has met all benchmarks specified in paragraph (c) of this section for all its applicable covered facilities, in which case the burden shifts to the petitioning 911 Authority. The Bureau may review the petition and determine whether to order the requested relief, issue a remediation order, or take other action as necessary.

(1) 911 Authorities may file petitions via the Public Safety and Homeland Security Bureau's Public Safety Support Center. The petition process shall be subject to the procedural requirements set forth in §§ 1.41, 1.45, and 1.47 of this chapter, and will be a restricted non-public proceeding.

(2) Prior to filing a petition, a 911 Authority must provide the covered 911 service provider with 30 days written notice, and the service provider shall have an opportunity to address the issue directly with the 911 Authority. If the issue has not been addressed to the 911 Authority's satisfaction within 30 days, the 911 Authority may file a petition with the Bureau Chief for relief, including the correspondence with the covered 911 service provider and all documentation on which to base a finding of lack of reasonableness. After receiving a petition, the Bureau Chief may issue an order at any time as specified in paragraph (e)(3) of this section, or take other intermediate actions as warranted.

(3) The petition must be in the form of an affidavit signed by a director or officer of the 911 Authority. The petition must contain all relevant facts and references to this rule section alleging a violation sufficient for the Bureau to make a determination or grant the requested relief.

(4) The covered 911 service provider may file an opposition to the 911 Authority's petition, and the 911 Authority may file a reply to the opposition in accordance with § 1.45 of this chapter. A copy of the document (petition, opposition, or reply) must be served on the other party (911 Authority

or covered 911 service provider) at the time of the filing in accordance with § 1.47 of this chapter.

(g) *Compliance dates.* Paragraphs (c) through (f) of this section may contain revised information collection and recordkeeping requirements that require review by the Office of Management and Budget. Compliance with paragraphs (c) through (f) of this section will not be required until this paragraph (g) is removed or contains a compliance date(s).

[FR Doc. 2025–09279 Filed 6–3–25; 8:45 am]

BILLING CODE 6712–01–P