April 2014 Multistate 911 Outage: Cause and Impact

REPORT AND RECOMMENDATIONS

Public Safety Docket No. 14-72
PSHSB Case File Nos. 14-CCR-0001-0007

A Report of the Public Safety and Homeland Security Bureau
Federal Communications Commission
October 2014

TABLE OF CONTENTS

FIGURES IN DOCUMENT

TABLE IN DOCUMENT

APPENDICES

1. INTRODUCTION AND EXECUTIVE SUMMARY

Just before midnight on Wednesday, April 9, 2014, Pacific Daylight Time (PDT) a 911 call-routing facility in Englewood, Colorado, stopped directing emergency calls to eighty-one 911 call centers (Public Safety Answering Points or PSAPs) in seven states – California, Florida, Minnesota, North Carolina, Pennsylvania, South Carolina, and Washington. The outage was caused by a software coding error in the Colorado facility, and resulted in a loss of 911 service for more than 11 million people for up to six hours. Over 6,600 calls to 911 never reached a PSAP. Although, fortunately, it appears that no one died as a result, the incident – and the flaws it revealed – is simply unacceptable. Americans rely on 911 as a reliable way to communicate in an emergency, and lapses like this cannot be permitted.

What is most troubling is that this is not an isolated incident or an act of nature. So-called "sunny day" outages are on the rise. That's because, as 911 has evolved into a system that is more technologically advanced, the interaction of new and old systems is introducing fragility into the communications system that is more important in times of dire need.

The April outage illustrates the problem. Following this incident, the Public Safety and Homeland Security Bureau (Bureau) investigated the causes and effects of the outage, relying upon confidential outage reports, public comments and related documents, as well as interviews of the relevant stakeholders, including service providers and public safety entities.[1] The Bureau also examined the record to identify ways to prevent such an outage from occurring again in the future.

In this report, the Bureau presents its findings. As discussed below, the outage was caused by a software coding error that prevented 911 calls from being processed timely and directed to the appropriate PSAP. It could have been prevented. But it was not.

The causes of this outage highlight vulnerabilities of networks as they transition from the long-familiar methods of reaching 911 to IP-supported technologies. In particular, the technical and operational failures that caused and prolonged the outage suggest the need for a close examination of the transition to IP-supported 911 services.

This has implications for the roll-out of Next Generation 911 (NG911). NG911 networks, which rely on IP-supported architecture rather than traditional circuit-switched time division multiplexing (TDM) architecture, introduce promising new capabilities, such as more flexible call routing and the ability to provide PSAPs with a greater range of information (such as video). At the same time, however, they can also introduce new vulnerabilities and challenges. For example, call control in legacy 911 networks was primarily performed in a central office switch that was close to the customers it served, whereas IP-supported networks increasing rely on geographically-remote

[1] The investigation into the circumstances of this incident was similar to that following the 911 outages resulting from the 2012 derecho storm. *See* FCC PUB. SAFETY & HOMELAND SEC. BUREAU, IMPACT OF THE JUNE 2012 DERECHO ON COMMUNICATIONS NETWORKS AND SERVICES: REPORT AND RECOMMENDATIONS at 4-5 (PSHSB, rel. Jan. 10, 2013), *available at* http://www.fcc.gov/document/derecho-report-and-recommendations (*Derecho Report)* (footnote omitted).

servers and software-based components to support key 911 functions, such as 911 call routing, across multiple states and jurisdictions. Consequently, a 911 outage in an IP-supported network has the potential to affect a much greater number of PSAPs and people, across multiple states, as demonstrated by the multistate effects of the April outage.[2] This outage also highlights the ongoing trend among communications providers and PSAPs to "contract out" 911 service functions to third-party vendors. This has concentrated critical functions in fewer locations that are more distant from the PSAP and the end user, and created a corresponding need to ensure such contractual arrangements do not compromise situational awareness and accountability for the end-to-end 911 call-to-completion process. Redundancy and responsibility are both endangered.

The introduction of NG911 and IP-based technologies will require industry as well as state, local, tribal and territorial governments and commissions to move aggressively to ensure that technology enabled optimization does not introduce unacceptable risks that threaten imperiling 911 reliability and resiliency. Everyone has a role in ensuring that 911 works as it should, when it is most needed.

The Federal Communications Commission (FCC or Commission) has a fundamental statutory responsibility to "promot[e] the safety of life and property through the use of wire and radio communications." [3] In light of this congressional mandate, ensuring the resilience of the nation's 911 system is a core value and public policy imperative.

2. Findings of Fact

2.1 Overview of the April 2014 Multistate Outage, and Parties Involved

As discussed below,[4] the Bureau analyzed information from a variety of sources, including confidential Network Outage Reporting System (NORS)[5] reports, interviews with service providers,

[2] While not an outage of a purely NG911 system, the software coding error that caused the outage occurred in IP-supported facilities that are part of the transition to NG911.

[3] 47 U.S.C. § 151.

[4] *See* Appendix B, "Information Gathering Process."

[5] Commission rules require that communications providers (e.g., wireline, wireless, cable, satellite, Voice over Internet Protocol (VoIP)) report major disruptions to voice communications to the Commission. The general threshold for reporting is an outage that potentially affects 900,000 user minutes and lasts at least 30 minutes. When an outage such as the April 2014 multistate outage affects or even potentially affects a PSAP, the provider is also required to contact the PSAP "as soon as possible" with "all available information." NORS is the Commission's mandatory, web-based filing system through which communications providers must submit reports to the FCC, and it is the primary means by which the Commission learns of significant outages. This system uses an electronic template to promote ease of reporting and encryption technology to ensure the security of the information filed. Network Outage Reporting System (NORS), http://transition.fcc.gov/pshs/services/cip/nors/nors.html. The Bureau's Cybersecurity and Communications Reliability (CCR) Division administers NORS, monitors the outage reports submitted through NORS, and performs analyses and studies of the communications disruptions reported. With the exception of interconnected VoIP service, a NORS Notification must be filed within 120 minutes of when a provider has discovered that the effects of an outage reach a certain threshold (*e.g.,* lasting at least thirty minutes and potentially affecting 900,000 user minutes). An Initial Report with additional information is due within 72 hours, and a Final Report with additional information is due within thirty days of the Notification. *See* 47 C.F.R. §§4.9, 4.11. The NORS team aggregates the data to identify outage trends.

PSAPs and state public service commissions and public comments. Based on its review of this record, the Bureau concludes that the April 2014 multistate outage was caused by a preventable software coding error in Colorado-based Intrado, Inc.'s (Intrado) Englewood Emergency Call Management Center (ECMC). Specifically, the software configuration error occurred in the Englewood critical call routing hub owned and operated by Intrado, a provider of 911 and emergency communications infrastructure, systems and services to telecommunications service providers and public safety agencies throughout the United States. This hub software was designed to keep track of the trunk assignment for 911 calls assigned to numerous PSAPs around the nation that (at some point in the architecture) relied on centralized automatic messaging accounting (CAMA) trunking, a legacy TDM type of trunk. When the software stopped making trunk assignments, it prevented calls being routed through the Englewood hub from reaching these PSAPs. Further, inadequate alarm management resulted in significant delays in determining the software fault and restoring 911 service to full functionality. Intrado operated a redundant hub in Miami, Florida to which 911 traffic could have been immediately rerouted, but because the malfunction was not detected promptly and mitigation actions were not efficiently developed, Intrado did not execute either an automatic or manual switchover of traffic to the Miami hub until six hours had elapsed. This switchover almost immediately restored the service.

Effects of the Outage. The preventable software coding error at Intrado's Englewood ECMC affected 81 PSAPs in seven states, including Washington, North Carolina, South Carolina, Pennsylvania, California, Minnesota, and Florida. During that time, over 6,600 calls to 911 nationwide were not delivered to the appropriate PSAP.[6] The effect was most drastic in Washington, where all the state's PSAPs were affected to some degree.[7] The affected counties have a combined population of 6,971,406,[8] and are served by dozens of primary PSAPs.[9] All of the people in Washington appear to have been without fully functioning 911 service for a period of up to six hours.

[6] Initial reports indicated that roughly 4,300 calls to 911 nationwide did not get through. *See* Reply Comments of the Washington State E911 Coordination Office ("Washington E911 Coordinator Reply Comments") at 2 ("During the outage, 700 911 calls were successfully delivered to the PSAPs, while approximately 4,500 911 calls failed."). *See also* CenturyLink Comments at 6 ("Approximately 4,453 calls in the States of Washington, Minnesota and North Carolina were impacted by the outage.") Those calls that were delivered to the appropriate PSAP went through Intrado's Miami, Florida, ECMC. Intrado has since updated the count, to clarify that over 6,600 calls to 911 nationwide did not get through. *See* E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado (Sep. 5, 2014). For more detailed discussion of the routing of calls from areas that Intrado serves either directly or as a third-party contractor, *see* Section 3 *infra.*

[7] *See* Pacific County Sheriff's Comments at 1 (filed Jun. 3, 2014) ("[I]t was quickly determined that the outage impact was statewide with the exception of two counties (Skamania County and Garfield County).") ("Pacific County Sheriff's Comments"). Since the Pacific County Sheriff's Office filed its comments, Intrado has informed the Bureau that its review of its own data indicates that all counties in the State of Washington were affected by the outage. *See* E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado (Sep. 5, 2014).

[8] *See* National Association of Counties; "Find a County," http://www.naco.org/Counties/Pages/FindACounty.aspx (accessed Jul. 18, 2014).

[9] *See* Washington E911 Coordinator Reply Comments at 2 (filed Jun. 30, 2014). "E911 service is provided to the public through 57 primary [PSAPs], including two federal installation PSAPs, one native American Tribal PSAP and four State Patrol PSAPs."

The multistate effects of the outage are shown in the table below:

	Total No. Consumers Possibly Affected	**PSAPs Affected**	**Counties Affected**
California	30,000	13	8
Florida	477,739	3	3
Minnesota	2,857,370	9	6
North Carolina	175,936	2	2
Pennsylvania	561,973	1	1
South Carolina	239,363	1	1
Washington	6,971,406	52	39
TOTAL	**11,313,787**	**81**	**60**

Table 1: Effects of Multistate Outage

Over 11 million Americans, then, or about three and half percent of the population of the United States, were at risk of not being able to reach emergency help through 911.

As of the release of this Report, Intrado reported[10] a total of 6,410 calls to 911 attempted, of which 5,618 failed in the Washington, North Carolina, and Minnesota, as described in the table below.[11] Approximately one-thousand additional calls failed in California, Florida, Pennsylvania, and South Carolina.

[10] Information contained in this report is no longer protected as confidential either because it is now in the public domain, e.g., through media reports, and/or the NORS-reporting provider has agreed to waive confidential protection with respect to those facts and assertions. Additional information in NORS reports and responses to information requests remains presumptively confidential under Section 4.2 of the Commission's rules. *See* 47 C.F.R. §4.2.

[11] *See* E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado (Sep. 12, 2014).

Call Type	**Attempted Calls**	**Failed Calls**	**Successful Calls**
VoIP	465	425	40
Wireless	3,598	3,555	43
Wireline	2,347	1,638	709
Total	**6,410**	**5,618**	**792**

Table 2: Failed Calls in Washington, Minnesota, and North Carolina

Based on the Bureau's investigation, it is not clear why a small number of calls were completed. The most likely reason is that those calls were routed through the Miami ECMC.

Providers Involved. The following is a description of parties that submitted NORS reports:[12]

Intrado. Colorado-based Intrado is a provider of 911 and emergency communications infrastructure, systems, and services to communications service providers and to state and local public safety agencies throughout the United States. Its commercial customers include wireline, wireless and VoIP providers, while it also serves as the direct 911 service provider for many PSAPs and 911 authorities. Intrado provides some level of 911 function for over 3,000 of the nation's approximately 6,000 PSAPs. In many cases, Intrado provides 911 services that traditionally have been performed by local telecommunications providers.

In broad terms, Intrado is either is the direct provider of 911 service to a jurisdiction (as it is with the State of Vermont and certain counties in Florida, Pennsylvania, and South Carolina) or the third-party contractor (as it is with CenturyLink in the States of Minnesota, North Carolina, and Washington, and with Verizon Business in the State of California).[13]

[12] AT&T Inc., while not affected or implicated in this outage, also filed a NORS Report. AT&T noticed that 911 calls were not being completed on other networks, and started receiving alarms relating to the outage by 2:20 a.m. PDT. At some point during that time interval, AT&T determined from an analysis of Signaling System No. 7 (SS7) messages from Intrado's network that 911 calls were timing out after reaching Intrado. This led AT&T to conclude that the problem was in Intrado's network. *See* E-mail from Joe Marx, Assistant Vice-President, Federal Regulatory, AT&T Inc., to Julia Tu, Cybersecurity and Communications Reliability (CCR), PSHSB (May 30, 2014).

[13] As this relationship illustrates, traditional incumbent local exchange carriers (ILECs) and other third party service providers have begun to enter into different contractual relationships with each other or with PSAPs, creating a need to ensure coordination between participants in ensuring the reliability of the provision of end-to-end 911 service.

CenturyLink. CenturyLink is under contract with Washington[14] to maintain the State's high-bandwidth Emergency Services IP Network (ESINet) as a managed network and to ensure proper routing, transport, interoperability and security of network traffic. In December 2013, CenturyLink announced that it had completed replacement of the State's analog, voice-grade 911 system with an ESINet that would enable infrastructure for future adoption of emergency communication services such as real-time text, video, voice and data messages from various types of devices. The PSAPs in all of Washington's 39 counties are connected to the ESINet.[15]

Relationship Between CenturyLink and Intrado. In 2004, Intrado and Qwest Corporation (predecessor-in-interest to CenturyLink) entered into a services agreement (Agreement), which was later amended to include provision of the NG911 services at issue in this matter.[16] The Agreement requires each party to comply, at its own expense, with all applicable federal, state, county and local ordinances, regulations and codes in the performance of its obligations under the Agreement.

Comcast and TCS. Comcast provides VoIP and other communications services to a small section of the State of Washington, and uses TCS as a VoIP Positioning Center (VPC) for its 911 traffic. TCS provides Comcast 911 call routing instructions at the time of an emergency call as well as Master Street Address Guide (MSAG) validation services as the VPC vendor. Comcast leverages this information from the TCS database to route its 911 traffic and deliver a pseudo ANI and shell record for a 9-1-1 caller. After delivery to the CenturyLink network, this information is used by the 9-1-1 center to query the TCS database and obtain the customer's call back number and address. TCS is able to monitor whether each 9-1-1 call routing request received from Comcast is followed by an automatic location identification (ALI) query from the receiving PSAP, as would typically occur on both E911 legacy and Internet Protocol Selective Router (IPSR) calls.

Verizon Business. Verizon Business is the 911 service provider for eleven counties in Northern California for 911 calls originating from AT&T Mobility and Verizon Wireless. Verizon Business subcontracts to Intrado for certain functions, including IP selective routing of 911 calls from these providers. Calls to 911 from AT&T Mobility and Verizon Wireless subscribers were affected by this outage. Verizon Business also provides an IP trial 911 network to these same PSAPs for calls originating with other providers. Calls to 911 in the trial areas from providers *other than* AT&T Mobility and Verizon Wireless use a different 911 network that was unaffected by the event in Intrado's network. This means that all wireline users, all VoIP users and customers of wireless providers other than AT&T Mobility and Verizon Wireless were not impacted by the outage.

[14] CenturyLink also provides 911 service within the States of Minnesota and North Carolina. *See* CenturyLink Comments at 1-2, and n.3. ("This same technical problem [at Intrado's ECMC] also caused limited CenturyLink 911 service outages in Minnesota and North Carolina during the same timeframe.") (footnote omitted).

[15] Source: *CenturyLink Upgrades Washington State's 911 Network to ESINet,* BELLEVUE BUSINESS JOURNAL, Dec. 12, 2013, available at http://bellevuebusinessjournal.com/2013/12/12/centurylink-upgrades-washington-states-911-network-to-esinet/ (accessed Aug. 12, 2014).

[16] See E-mail from Stacy Hartman, Director – Federal Public Policy, CenturyLink, to Jeffery Goldthorp, Acting Chief, Cybersecurity and Communications Reliability Division, PSHSB (Jul. 7, 2014), "Agreement for Services Between Intrado Inc. and Qwest Business Resources, Inc." (Mar. 1, 2004).

No PSAPs served by Verizon Business noticed the outage at the time it occurred.[17] PSAP officials first became aware of the impact on the public in their area when Bureau staff contacted them in the course of this investigation.[18]

AT&T Mobility (Cingular): AT&T Mobility is one of several wireless providers in the State of Washington. AT&T Mobility indicates that its network experienced E911 failures in the Tacoma, Washington, area, and that service was restored when CenturyLink restored circuits to the 911 network.

Frontier: Frontier is a local exchange carrier that provides service to both residential and business customers in Washington. All of Frontier's landline customers in the affected territory received busy signals when dialing 911.[19]

2.2 Timeline of Events During the Outage

The normal routing of 911 calls in the NG911 transition architecture that is discussed in this report is treated more fully in Section 3.

At 11:54 p.m. PDT[20] on April 9, 2014, the PSAP Trunk Member's (PTM) counter at Intrado's Englewood, Colorado, ECMC exceeded its threshold and could send no more 911 calls to PSAPs using CAMA trunks. Under normal operations, the PTM assigns a unique identifier for each call that terminates using CAMA trunks. This is how Intrado has implemented the ATIS protocol commonly used to complete 911 calls over CAMA trunks, which (unlike SS7) require additional features to carry the signaling along the TDM path.[21]

In this case, the trunk assignment counter reached a pre-set capacity limit to assign trunks, which meant that no additional database entries to reserve a PSAP CAMA trunk could be created, no trunk assignments for call delivery could be made for PSAPs with CAMA trunks[22] and, therefore, no 911 calls could be completed to these PSAPs or any backup PSAP through the Englewood ECMC.

At 12:54 a.m. PDT on April 10, 2014, a full hour after the counter had reached its threshold, low-level alarms began to go off at the Englewood, Colorado ECMC. The alarms were automatically

[17] *See, e.g.*, CCR Telephone Interviews with: Eric Ewing, Chief, Lassen County Office of Emergency Services (Aug. 12, 2014); Rick Andresan, Yreka Police Department (Aug. 12, 2014); Janice Grant, Public Safety Dispatch Supervisor, Sutter County Sherriff's Office 9Aug. 12, 2014).

[18] *See, e.g.*, CCR Telephone Interview with Eric Ewing, Chief, Lassen County Office of Emergency Services (Aug. 12, 2014).

[19] CCR Telephone Interview with Vicky Oxley, Vice-President & General Manager for the State of Washington, Frontier, *et al.* (May 19, 2014).

[20] Unless otherwise specifically noted or clarified, all times listed in this document are Pacific Daylight Time (PDT).

[21] *See* Request for Assistance Interface Specification – American National Standard, ATIS-0500019.2010, September 2010.

[22] *See* Comments of CenturyLink at 5 ("CenturyLink Comments") (filed Jun. 16, 2014) in PS Docket No. 14-72.

categorized by the server monitoring logs as "low level," and personnel at the ECMC appear to have realized neither what had failed nor the severity of the problem.[23] The low-level designation was a default setting accepted by Intrado's System Administrator that, in hindsight, did not reflect the potential severity of the fault. In the first few hours, Intrado was responding to a series of individual PSAP incidents and an area network outage in Oregon that was later determined unrelated. It appears that Intrado was not able to fully understand the significance and breadth of the problem until around 2:00 a.m. PDT,[24] when CenturyLink[25] informed it that CenturyLink's PSAP customers in the State of Washington were suffering an outage.[26]

Frontier became aware of the outage at 1:35 a.m. PDT, when it received a call from the Benton County (WA) PSAP that some 911 calls were not getting through. Shortly thereafter, Whitman and Ferry Counties also indicated that 911 calls were not getting through. When 911 calls from Frontier's customers reach CenturyLink's system, Frontier does not have visibility into either CenturyLink or Intrado's systems. All of Frontier's landline customers in Washington heard busy signals when they called 911.[27]

TCS notified Comcast of the outage at 2:45 a.m. PDT.[28] A Comcast engineer had noticed irregularities in alerts in a Comcast network operations center (NOC), but had not yet concluded that there was a problem when the call from TCS arrived.[29] On the morning of April 10, a TCS system noticed that it was receiving significantly fewer ALI queries than there had been call routing requests by Comcast, and that triggered an alarm for TCS.[30] Comcast and TCS arranged to reroute Comcast customer 911 calls to the TCS Response Center (TRC).[31] According to TCS, the TRC "is an emergency call center service offered to [VoIP service providers] who need an added level of call delivery backup. The TRC takes subscriber calls for emergency assistance that do not successfully route through the normal call flow. As a 9-1-1 call center that is capable of providing nationwide 9-

[23] *See* CenturyLink Comments at 5 ("These alarms were delivered, but the alarms were not specific nor was the appropriate severity clear to Intrado.")

[24] *See* E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado, Confidential Response Attachment 1, "Timeline of Events" (Jul. 10, 2014).

[25] CenturyLink contracts with Intrado for the latter to provide 911 services in, *inter alia*, Washington, Minnesota, and North Carolina. We discuss the contractual relationships between the parties, and the ramifications of such contracts, more fully and in detail at Section 2.1 *supra.*

[26] *See* CenturyLink Comments at 7 ("CenturyLink was notified of the outage by one of its PSAP customers in Washington . . . CenturyLink informed Intrado of the outage.")

[27] CCR Telephone Interview with Vicky Oxley, Vice-President & General Manager for the State of Washington, Frontier, *et al.* (May 19, 2014).

[28] CCR Telephone Interview with Mary P. McManus, Senior Director, FCC Policy, Comcast, *et al.* (May 20, 2014); CCR Telephone Interview with Tim Lorello, Senior Vice-President and Chief Marketing Officer, TeleCommunications Systems, Inc. (TCS), *et al.* (May 16, 2014). *See also* TCS and Comcast NORS Reports.

[29] CCR Telephone Interview with Mary P. McManus, Senior Director, FCC Policy, Comcast, *et al.* (May 20, 2014).

[30] CCR Telephone Interview with Tim Lorello, Senior Vice-President and Chief Marketing Officer, TeleCommunications Systems, Inc. (TCS), *et al.* (May 16, 2014).

[31] CCR Telephone Interview with Mary P. McManus, Senior Director, FCC Policy, Comcast, *et al.* (May 20, 2014).

1-1 dispatch, the TRC ensures that [the VoIP service provider has] a safety net for calls that need human hand-holding in the event that they cannot be automatically routed."[32]

NORS reports showed that Intrado had redundant capability to reroute 911 traffic through its Miami ECMC, but the Englewood outage was a "silent failure" that, due to a "low-level fault" designation, did not trigger automatic rerouting. Moreover, for several hours Intrado was unable to identify the root cause of the failure to deliver 911 calls to the appropriate PSAP. For at least a portion of that time, Intrado and CenturyLink were also dealing with a separate and simultaneous 911 outage on CenturyLink's network in northern Oregon, leading to a misdiagnosis of the actual problem for a period of that time.[33] The Oregon outage ultimately proved unrelated to the Washington outage, but for several hours early on April 10, Intrado and CenturyLink worked under the mistaken impression that the Washington and Oregon outages were related. As Intrado noted in its publicly-filed reply comments, this diverted its attention from the true cause of the multi-state outage.[34]

After the problem was identified, Intrado personnel performed a manual switch to reroute 911 calls to the Miami ECMC to restore 911 call processing.

3. OUTAGE IMPACTS ON 911 CALLS AND NETWORKS

This section discusses the causes of the outage and possible ways to avoid recurrences of similar outages. The section is divided into four subsections:

- Description of Washington State E911 Architecture
- Root Causes
- 911 Operations and Maintenance
- 911 Service Providers' Action to Prevent Recurrence.

3.1 Description of Washington State E911 Architecture

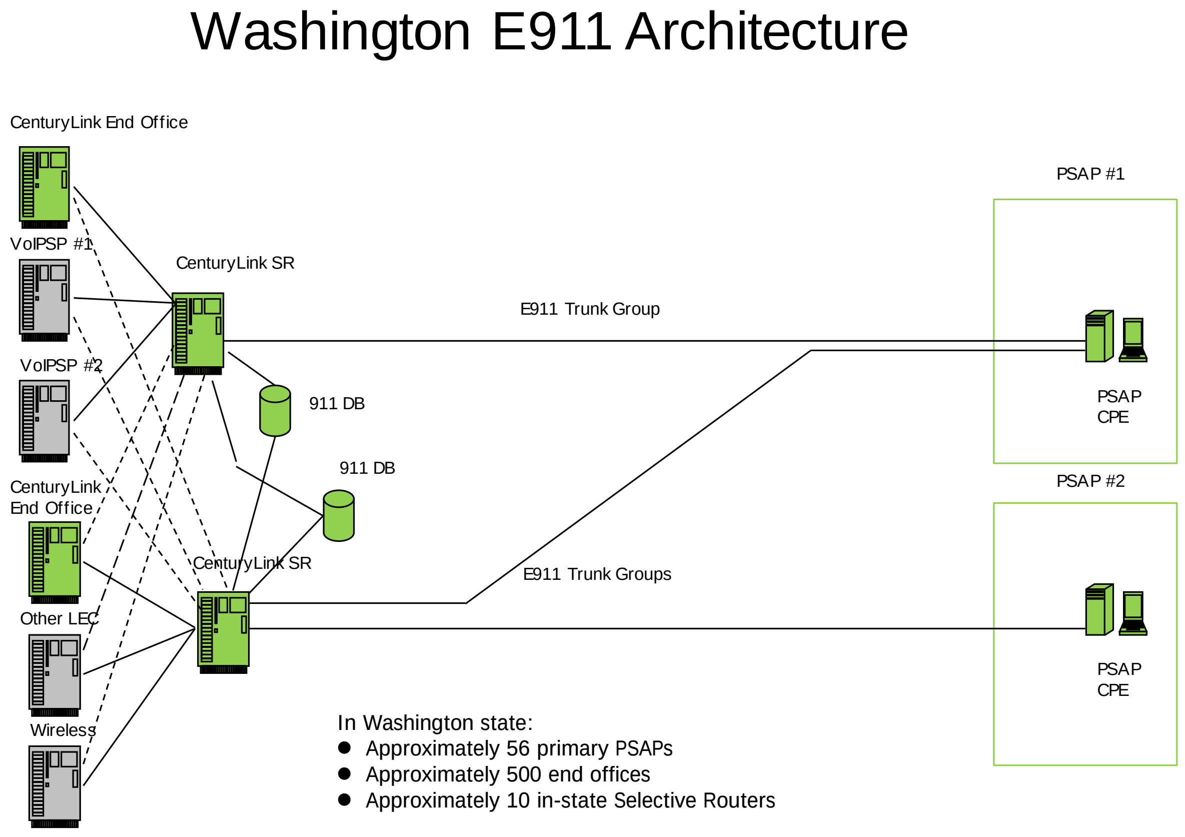
The following discussion describes the 911 architecture for the State of Washington on the day of the outage, as well as that state's evolution from conventional E911 to the current architecture,

[32] TCS, "911 Call Center Service," web page, available online on July 25, 2014, at http://www.telecomsys.com/products/public-safety/911-call-center-service.aspx.

[33] *See* CenturyLink Comments at 2 n.3. "In addition to the outage affecting Washington, Minnesota and North Carolina, on April 10, 2014 CenturyLink experienced a separate 911 outage that affected approximately 16,000 people in 3 Oregon counties for 3 hours and 26 minutes due to a maintenance issue unrelated to the [Intrado] equipment issue discussed throughout the majority of this filing." *See also* Reply Comments of Intrado at 6-7 ("Intrado Reply Comments") (filed Jun. 30, 2014).

[34] *See* Intrado Reply Comments at 7 ("Intrado spent precious time investigating reports that the CenturyLink outage [in Oregon] was or might be related to the [multistate 911] outage, causing technicians to reach invalid conclusions until finally eliminating the CenturyLink 911 outage [in Oregon] as a cause or partial cause. This contributed to the delay in diagnosing the real issue underlying the outage and thus increased the duration of the outage. There was also inconsistent communication between Intrado and the PSAP community which contributed to confusion and failure to incorporate critical information into Intrado's diagnosis.").

which is a transitional stage toward NG911. While the April 2014 outage affected communities in multiple states across the country, the scale and totality of the impact is dramatically illustrated by the experience in the State of Washington, where every citizen's ability to reach 911 was impaired. Neighboring PSAPs that, in the past, could have contributed to continuity of operations plans through mutual aid agreements were also down due to the centralized nature of the IP 911 database architecture. To the extent that this report focuses on the impact of the outage on Washington, such focus is not meant to exclude other jurisdictions, but rather reflects the reality that a 911 system of an entire state was not, for all intents and purposes, fully functioning.



In Washington state:
- Approximately 56 primary PSAPs
- Approximately 500 end offices
- Approximately 10 in-state Selective Routers

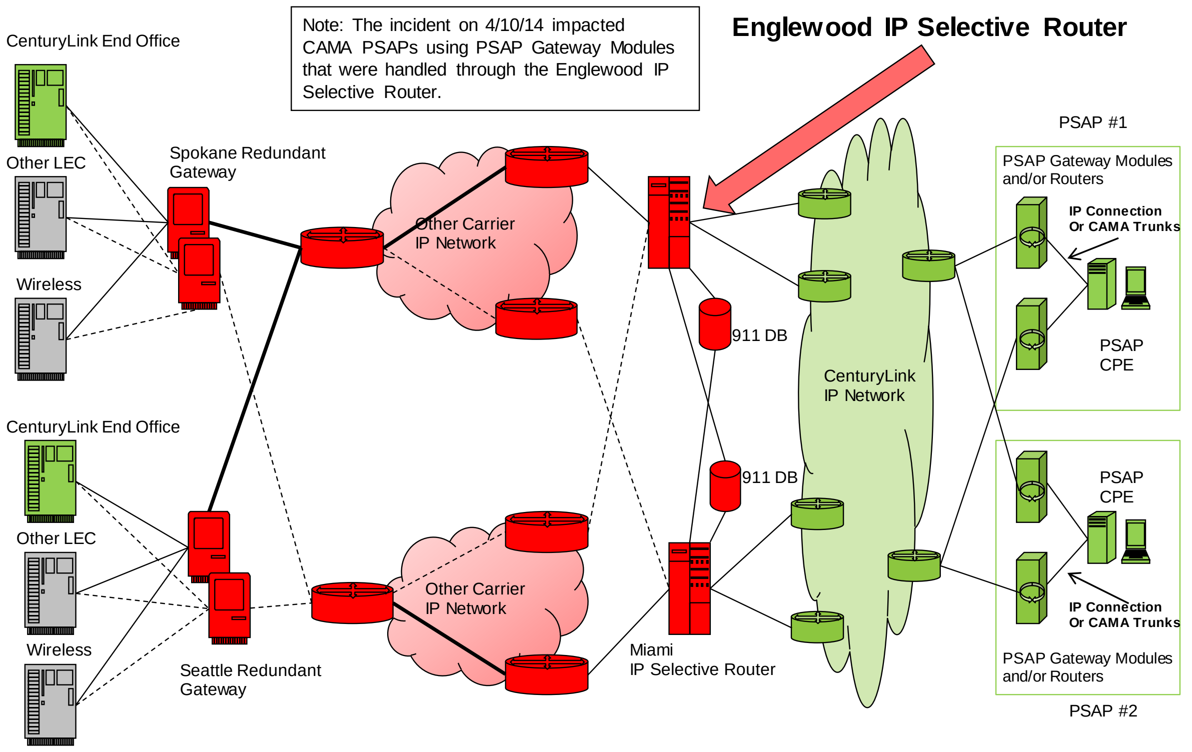
Figure 1: Washington Conventional E911 Architecture

Figure 1 above illustrates the legacy E911 architecture away from which Washington began to migrate in 2009.

With legacy TDM E911, as shown in Figure 1, a caller dials 911, and the call is routed through the network of its originating provider to a CenturyLink Selective Router (SR) based solely on the dialed number – 911. The SR is a telephone company central office switch that is "911-aware," *i.e.,* it knows that it cannot determine the route to the correct PSAP solely from the dialed number, but must also take into account the caller's location in order to route to the PSAP that serves that location. To do this, the SR refers to other databases, potentially in another state, to determine the E911 trunk group to the correct PSAP. It then routes the call onto that trunk group, which then completes the call to the PSAP.

In Figure 1, PSAP #1 is "dual-homed," *i.e.,* has trunks to more than one SR for improved reliability. This is not uncommon, but not all PSAPs throughout the United States are connected to redundant SRs.

Washington NG911 Transition Architecture


Note: The incident on 4/10/14 impacted CAMA PSAPs using PSAP Gateway Modules that were handled through the Englewood IP Selective Router.

Englewood IP Selective Router
CenturyLink End Office
Other LEC
Wireless
Spokane Redundant Gateway
Other Carrier IP Network
911 DB
CenturyLink IP Network
PSAP #1
PSAP Gateway Modules and/or Routers
IP Connection Or CAMA Trunks
PSAP CPE
CenturyLink End Office
Other LEC
Wireless
Seattle Redundant Gateway
Other Carrier IP Network
911 DB
Miami IP Selective Router
PSAP CPE
IP Connection Or CAMA Trunks
PSAP Gateway Modules and/or Routers
PSAP #2

911 call control, voice and ALI packets travel from WA, to FL or CO, and back to WA

- Multiple IP providers involved in multiple states

Figure 2: Washington NG911 Transition Architecture

Figure 2 above, adapted from a diagram provided by CenturyLink, depicts the Washington state 911 network as it existed on April 9-10, 2014 and as it exists currently.[35] It represents a step along the

[35] Graph provided by CenturyLink, "Next Generation 911 System Major Outage Report, RE: April 10, 2014 system outage," April 24, 2014, available online on June 23, 2014, available in .docx format at http://www.wutc.wa.gov/rms2.nsf/177d98baa5918c7388256a550064a61e/2ebf520dd09af01088257cc4008108eb!OpenDocument or in .pdf format at http://www.wutc.wa.gov/rms2.nsf/177d98baa5918c7388256a550064a61e/fde2bea93f21629888257cc400810915!OpenDocument .

transition path between conventional E911 and true NG911.[36] Here, a caller dials 911, and the call is routed through the network of the originating service provider to one of four Intrado gateways serving Washington State, two in the Seattle area (western Washington State), and two in the Spokane area (eastern Washington State). This gateway, which converts the signal from TDM to IP, is also 911-aware and queries other databases to determine the primary Internet Protocol Selective Router (IPSR) for the PSAP that serves the caller's location. Under normal conditions, the gateway then routes the call to the primary IPSR through a managed IP network, some of which belongs to CenturyLink and other parts of which are provided for those purposes by Intrado.[37] The IPSR is also 911-aware. As in the conventional E911 architecture depicted in Figure 1, it queries various databases (shown as "911 DB" in Figure 2) to identify the correct PSAP and to properly address packets to that PSAP. The call is then routed through the "CenturyLink IP Network" to the PSAP. The IPSR is no longer located in the local exchange carrier (LEC) central office, or even in Washington State, but is now in Colorado, with a single "manual failover" backup in Florida. As is often the case in conventional E911 architecture, databases are also located in other states.

The architecture in Figure 2 relies on more equipment than that depicted in Figure 1. This has important implications for network reliability, in that with more pieces of equipment (here, gateways in Seattle or Spokane; IPSRs; and/or gateways in or near the PSAP premises) handling each call and more stages, there is a greater chance for a 911 call to fail.

3.2 Root Causes

The Bureau's inquiry sought to understand the cause or causes of the April 2014 outage; why the outage affected so many PSAPs in such geographically-disparate places; and why the outage lasted as long as it did. At its most basic level, the multistate outage occurred because of a preventable software coding error in Intrado's equipment at the Englewood ECMC. The problem at Intrado's Englewood ECMC stopped non-IP-enabled trunk assignments, preventing calls being routed there from reaching the appropriate PSAPs. Moreover, the outage was prolonged because of: (1) deficiencies in Intrado's alarm processes; and (2) poor communications between Intrado and the parties with which it contracts to provide 911 services. Finally, the enormous breadth of the outage was in part attributable to an architecture that consolidated critical 911 functions in two locations serving multiple states, without adequate safeguards in place. While this consolidation lowered the cost of 911 operations for the LEC, the outage clearly showed that consolidation can result in too much dependence on a few critical elements if providers do not ensure the effective operation of adequate diversity and redundancy in the design and execution of the network.

As noted above, an IPSR is a 911-aware device that, under normal conditions, receives 911 calls from originating service providers, determines the correct PSAP for routing each call, and addresses the call to that PSAP. However, in those cases where the PSAP receives calls over TDM CAMA

[36] True NG911 refers to NG911 as defined by NENA in its various standards documents, especially the so-called i3 detailed requirements specification, the "Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3," issued June 2011, *available at* https://www.nena.org/?page=i3_Stage3.

[37] Under conditions outside the ordinary, for example, if the primary IPSR has failed, the gateway should route the call to the other IPSR.

trunk interfaces, the IPSR also assigns each call to a CAMA trunk interface. This assignment function is carried out by the PTM software module, which notes each CAMA trunk assignment in an activity log and assigns a log record number.

When it originally designed the software for its PTM, Intrado programmed it with a pre-set maximum of sequential log record numbers. At around midnight on April 9, the PTM module in Intrado's Englewood IPSR reached this maximum, at which point it ceased generating additional CAMA trunk assignments[38] for incoming 911 calls. When subsequent requests for CAMA trunk assignment were received, the PTM did not respond, interfacing timers timed out, and 911 calls were no longer completed to those PSAPs with CAMA trunks. In other words, these calls destined for PSAPs using CAMA trunks went nowhere. This amounted to over 87 percent of all 911 calls during the outage.

Notably, the IPSR did not issue any major or critical alarm for this outage.[39] Instead, it issued several thousand minor alarms for calls not completing, but these did not attract the attention of Intrado staff. As a result, all calls to CAMA-based PSAPs that were routed via Englewood failed until Intrado staff identified the problem at approximately 6:00 a.m. PDT on April 10.[40] Upon identifying the issue, Intrado initiated a manual failover to its alternate IPSR in Miami and subsequently began routing all of its incoming 911 calls to its Miami IPSR instead of the Englewood IPSR, until the software in Englewood was repaired several hours later.

3.3 911 Operations and Maintenance

While the technical cause of this multistate outage rested in Intrado's network, operations and maintenance for 911 communications generally was distributed among multiple communications providers. This complicated the process of detecting and repairing problems.

Figure 3 below, prepared by the Bureau, provides a generic E911 architecture (without IPSRs), and is a straightforward generalization of Figure 1.[41]

[38] We note that this incident was limited to CAMA trunk assignment; IP-enabled trunks processed through the Englewood ECMC were not affected by the multistate outage.

[39] *See* Washington E911 Coordinator Reply Comments at 4. ("The failure did generate an alarm, but the alarm was not distinguishable as a failure to process calls. Because of this, [Intrado] did not recognize the significance of the problem. In addition, even though the device that failed sent 4,500 alarms to [Intrado's Englewood office], they were grouped together in a summary, so again, the significance of the problem was not recognized by [Intrado].") *See also* CenturyLink Comments at 5 ("CenturyLink understands that Intrado has alarms in place to monitor the PTM. These alarms were delivered, but the alarms were not specific nor was the appropriate severity clear to Intrado.").

[40] CenturyLink informed Intrado that there was an as-yet-unidentified problem with Intrado's system at about 1:00 a.m., April 10. *See* CenturyLink Comments at 6 ("[o]nce the problem was properly diagnosed [at approximately 6:00 a.m.], Intrado initiated manual failover of all call processing to the Miami ECMC.")

[41] In order for the discussion that follows to include states other than Washington, and in order for it to include true NG911, we will generalize Figures 1 and 2 to be representative of all (or almost all) states' conventional and NG911 architectures, respectively.

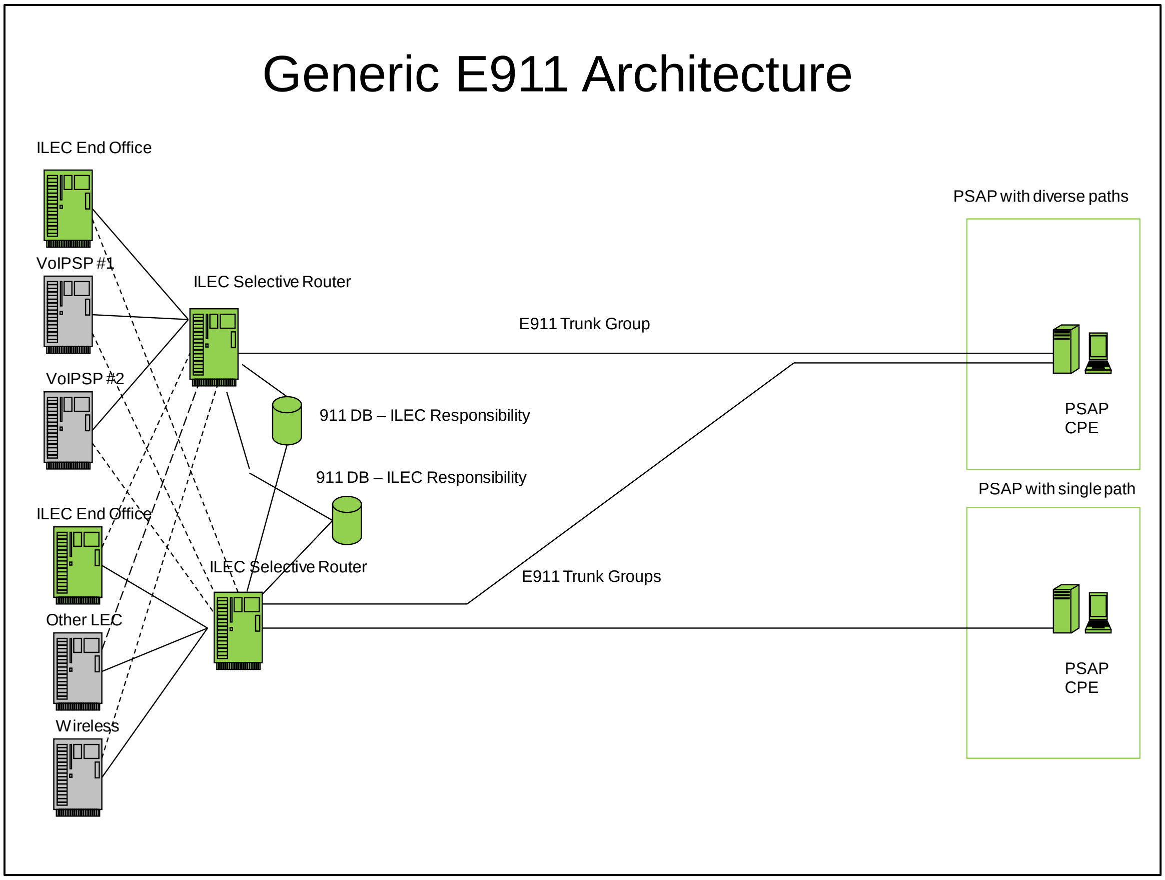


Figure 3: Generic Conventional E911 Architecture

In Figure 3, a TDM 911 call may be viewed as traversing three sections (not including PSAP customer-premises equipment (CPE)):

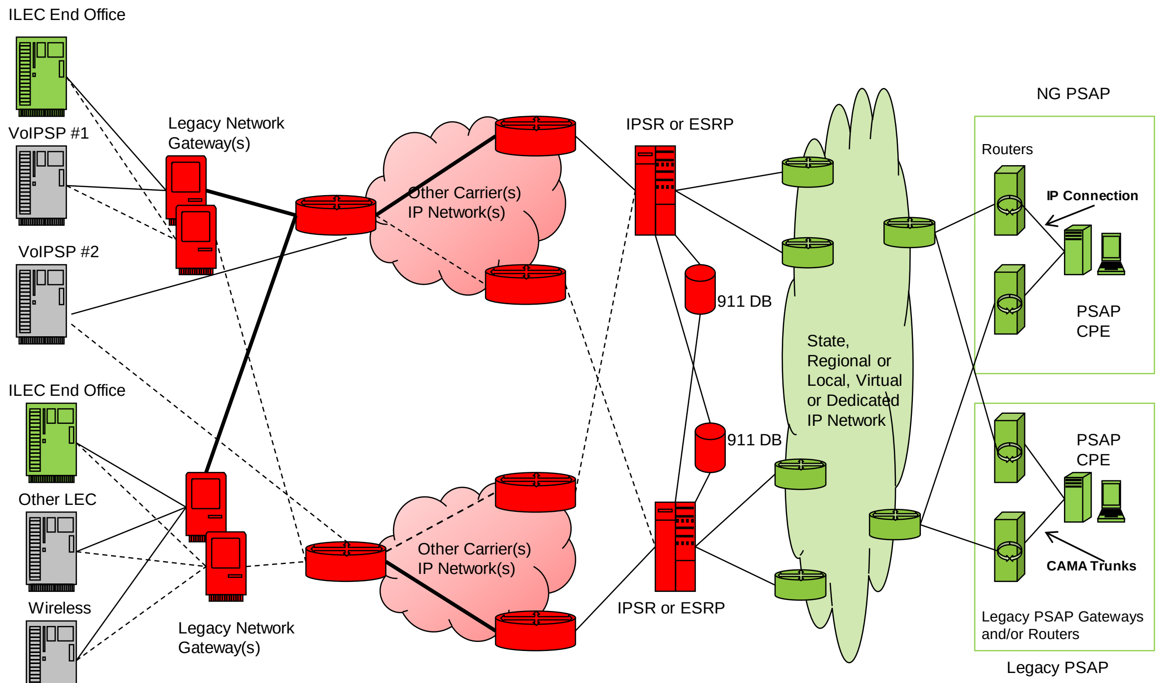
- **The section between the caller and the SR**, not including the SR. Calls are processed through service provider networks, and the incumbent local exchange carrier (ILEC) and other providers provide normal voice network maintenance in these networks.

- **The SR.** This is a 911-aware voice switch. Although it has selective routing features that most switches do not have, the SR switch is nonetheless designed to detect its own common equipment troubles in support of its maintenance.

- **The trunk(s) between the SR and the PSAP CPE** (including per-customer equipment in the SR line card). All of this is dedicated to one PSAP. If a PSAP loses its service, the covered 911 service provider (today, generally the ILEC) that operates the SR should detect outages and restore service and comply with applicable contract and tariff requirements.

Figure 4 illustrates both the NG911 transition architecture and the true NG911 architecture for completing calls from customers served by TDM networks:

Generic IPSR or NG911 Architecture


ILEC End Office
VoIPSP #1
VoIPSP #2
ILEC End Office
Other LEC
Wireless
Legacy Network Gateway(s)
Legacy Network Gateway(s)
Other Carrier(s) IP Network(s)
Other Carrier(s) IP Network(s)
IPSR or ESRP
IPSR or ESRP
911 DB
911 DB
State, Regional or Local, Virtual or Dedicated IP Network
NG PSAP
Routers
IP Connection
PSAP CPE
PSAP CPE
CAMA Trunks
Legacy PSAP Gateways and/or Routers
Legacy PSAP

In general, 911 call control, voice and ALI packets travel from the caller, to IPSR and ESRP locations, and back to the PSAP

- Multiple IP providers involved in multiple states

Figure 4: Generic IPSR or NG911 Architecture

Where Figure 2 showed an IPSR, Figure 4 shows "IPSR or ESRP." An Emergency Services Routing Proxy (ESRP) is, like an IPSR, a 911-aware device that can route calls to the correct PSAP based on the caller's location. The ESRP provides this function in true NG911. SRs, IPSRs, and ESRPs all utilize external databases and location systems to determine the correct route. However, SRs and IPSRs use E911 databases and location systems, while ESRPs use NG911 standardized databases and location systems.

In Figure 4, as in Figure 3, a 911 call may be viewed in distinct sections for maintenance planning purposes. Those sections (not including PSAP CPE) are:

- **The section between the caller and the Legacy Network Gateway (LNG)**, not including the LNG. Calls are processed through the caller's service provider network. (In Figure 4, for VoIP Service Provider #2 (VoIPSP #2), this section would not include the LNG, but instead would correspond to the section between the originating network and the managed "Other Carrier IP Network," not including the latter.)

- **The section that includes the LNGs, the IPSRs or ESRPs, and the Legacy PSAP Gateways (LPGs), and interconnecting IP networks.** This section routes 911 calls to a group of PSAPs. This part of the architecture replaces the Selective Router and the E911 trunk groups in Figure 3.

3.4 911 Service Providers' Actions to Prevent Recurrence

The discussion below describes some of the actions taken to restore service in the immediate aftermath of the outage, as well as steps taken to prevent recurrence of similar outages and/or mitigate their impact.

Intrado:

Intrado implemented a number of new features to fix the original problem with the PTM and to prevent recurrence of the same or similar problems. The most important changes include:

- Significantly increasing the PTM counter limit for both ECMCs (*i.e.*, in Englewood and in Miami) to reduce the possibility of reaching the maximum threshold, and checking the PTM counter value weekly to ensure the value is not nearing the higher, maximum threshold;

- Creating an alarm "based on percentage of successful calls processed on a given ECMC compared to total calls for that ECMC over a 15-minute sample period." Thus, in the future, whenever the ECMC stops processing calls, regardless of the reason, the failure should generate an immediate alarm; and

- Implementing a change to automatically reroute an individual call to another ECMC if for some reason that call cannot be processed at its primary ECMC. This change permits 911 calls in the NG911 transition architecture to route to an available server as is commonly found in a distributed Internet service.[42]

Had these changes been in effect on April 9-10, this specific outage most likely would not have occurred.

Appendix D contains a table, provided by Intrado, documenting these and other system changes that it has made to repair the failure that caused the multistate outage and to prevent recurrence.

CenturyLink:

CenturyLink has described steps that it is taking to avoid similar problems:

[42] *See* E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado (Jul. 10, 2014). Note that in the table, ECMC refers to Intrado's Emergency Call Management Complexes in Miami and Englewood.

> . . . Intrado and CenturyLink will engage in a NOC-to-NOC partnership session to work through NOC-to-NOC challenges and establish or clarify process changes. While Intrado and CenturyLink had outage handling procedures in place prior to this event, they have since adopted additional procedures such as the establishment of a joint technical bridge, a modified escalation process, and an outage and event group email notification. Intrado and CenturyLink will also jointly review the ingress trunking configuration distribution between ECMC processing sites. Intrado and CenturyLink are also jointly reviewing the current architectural design to assess potential improvements for even greater resiliency.[43]

CenturyLink added that, while the April 2014 outage was not caused by any failures or malfunctions in equipment other than as provided by Intrado, it is determined to remain vigilant to ensure the utmost reliability and resiliency of the 911 network.[44] We would expect such vigilance would extend to ensuring contractually that its contractors are obligated to do the same.[45]

3.5 Impacts on Public Safety Answering Points

In total, this outage affected 81 PSAPs served by legacy CAMA trunks, as the counter that failed in Intrado's ECMC was used in making assignments of these types of trunks. While a PSAP that was made aware of a 911 service outage traditionally may have rerouted service to an alternate PSAP, this action would have been no guarantee of service restoration in this situation, because in many cases, the alternate PSAP (also served by CAMA trunks) was using the same ECMC and was therefore also experiencing a 911 service outage.

All of Washington State's 39 counties were affected by the multistate outage.[46] The Bureau conducted in-depth conference calls with PSAP officials in seven representative counties covering 19 PSAPs (Benton, Columbia, Cowlitz, Jefferson, King, Snohomish, and Thurston) to gather more information on how they were affected.[47] All of these PSAPs use CenturyLink as their primary 911 provider and are part of the statewide CenturyLink-operated ESInet network.[48]

[43] *See* CenturyLink Comments at 8-9.

[44] *See* CenturyLink Comments at 9.

[45] The Bureau does not have information as to whether other 911 service providers with similar configurations and contractual arrangements have made revisions to avoid the issues addressed in this report.

[46] *See* Pacific County Sheriff's Comments at 1; E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado (Sep. 5, 2014). While the outage affected many jurisdictions throughout the United States, its impact was felt was dramatically and overwhelmingly in the State of Washington, where the ability of all citizens there was impaired. To the extent that this report would appear to focus on the impact of the outage on Washington, such focus is meant not at the exclusion of other jurisdictions but rather reflects the reality that a 911 system of an entire state was, for all intents and purposes, not fully functioning.

[47] The counties listed are a representative sampling of densely-populated urban area, rural, and mid-sized cities.

[48] The State of Washington, through its Military Department, has a contract with CenturyLink for the latter to be "the sole wireline 911 service provider for the State of Washington and has partnered with Intrado to provide this service. The contract was executed between Qwest and the State of Washington in 2008 and effective in 2009. Service was turned up in 2009 and a transition began at that time from legacy 911 to Emergency Services IP Network ("ESINet")." See CenturyLink Comments at 3-4.

Because the outage occurred in Intrado's network, and PSAPs had no contractual relationship with Intrado, CenturyLink was the primary interface for the PSAPs.[49] Because CenturyLink contracted for 911 database service from Intrado, however, CenturyLink was unable to mitigate the outage directly and was subject to the architectural decisions made by Intrado. Reroutes, the most common service restoration method for PSAPs, would not have worked in this case because the 911 calls were generally rerouted to alternate PSAPs that were also affected by the outage at Intrado's Englewood ECMC.

Analysis of NORS data reveals that, compared to the extent of the outage in Washington State, the effects in other states were considerably less widespread, from both a geographic and population standpoint. PSAPs in Minnesota, Florida, Pennsylvania, North Carolina, South Carolina and California were affected by the April 2014 outage. After having discussed the outage with numerous Washington State-based PSAPs, Bureau staff continued its inquiry with a subset of PSAPs in those states. Based on its discussions with these PSAPs, the Bureau determined that the cause of the multistate outage was the same as in Washington State (*i.e.*, the ECMC issue at Intrado's Englewood office), and the effects were similar.

As noted below,[50] many PSAPs in the affected areas stated that they received no notification from ILECs or Intrado about this outage. Where information was received, some of those PSAPs believed that it was deficient, and claim that no useful information was imparted to the PSAPs. PSAPs in Washington State, for example, stated that neither CenturyLink nor Intrado communicated with them to assess status either during or immediately after the event.[51]

Some PSAPs also informed the Bureau that during the outage, they took the initiative to reach out to CenturyLink, but were kept on hold.[52] For example, the Columbia County (WA) PSAP stated that it learned of the problem when it received a call from the Washington State E911 Advisory Committee at 2:33 a.m. on April 10. Snohomish County reported that CenturyLink sent mass e-mails to PSAPs at about 3:00 a.m. throughout the state, but that many of these e-mails included incorrect addresses and never reached the intended recipients.[53] CenturyLink counters that it did, in fact, reach out to both individual PSAPs and the state-wide E911 agency to give PSAPs situational awareness. Specifically, it states that:

[49] As noted above, while Intrado is the third-party contractor in the State of Washington and does not have any direct relationship to PSAPs there, it is direct provider of certain 911 services in other jurisdictions (*e.g.,* the State of Vermont, certain counties throughout the nation).

[50] *See* Appendix B, "Information Gathering Process."

[51] *See, e.g.,* CCR Telephone Interview with Lisa Caldwell, Columbia County 911 Coordinator (May 7, 2014).

[52] *See, e.g.,* CCR Telephone Interview with Jim Barber, Manager, and Doug deGraaf, Information Systems Manager, Benton County Emergency Services (on hold for 30 minutes); CCR Telephone Interview with Karl Hatton, 911 Coordinator, Jefferson County (on hold 30 minutes); CCR Telephone Interview with Curt Mills, Executive Director, SNOPAC 911, Snohomish County, Washington, *et al.* (on hold for 30 minutes before hanging up without having spoken with anyone from CenturyLink).

[53] CCR Telephone Interview with Curt Mills, Executive Director, SNOPAC 911, Snohomish County, Washington, *et al.* (May 5, 2014)

> [u]pon receiving trouble reports from PSAPs, the CenturyLink 911 Repair Center notified Intrado at 12:58 a.m. (PDT). At this point, CenturyLink began calling PSAPs in the area, while also fielding a flood of calls. . . . Additionally, the Washington State E911 Coordinator's Office created a bridge and sent an email to the distribution of PSAP Coordinators to join. The CenturyLink Washington Service Manager provided periodic status and restoration updates on this bridge.[54]

4. POLICY IMPLICATIONS OF THE APRIL 2014 MULTISTATE 911 OUTAGE

The multistate outage raises a number of issues regarding the deployment of transitional and NG911 systems. Although the specific nature of the software limitation is well understood, and Intrado has endeavored to ensure this specific event does not recur, the outage revealed larger concerns about possible vulnerabilities in NG911 system architecture designed without adequate redundancy, diversity, and adherence to operational best practices.

NG911 systems rely on IP-supported architecture rather than the public switched telephone network (PSTN)-based architecture of legacy 911. This IP-supported architecture allows the introduction of new functional and logical intelligence into the end-to-end 911 system and enables support for an expanded array of emergency communications services. Necessarily, NG911 system architecture takes into account the need to preserve certain core legacy 911 functionalities, given legacy networks on which 911 callers continue to rely, at the same time it enables new IP-supported call handling functions. When implemented properly, NG911 architecture can offer distinct advantages over legacy technologies, including the possibility of greater redundancy and reliability. For example, in the Derecho Report, the Bureau concluded that if NG911 architectures and capabilities had been in place in the areas affected by the derecho storm, the storm would likely have had less of a negative impact on emergency communications.[55]

4.1 Shifting of Critical Operational Functionality

With the transition to NG911 system implementation, new entrants have already begun to enter the market for the provision of key functional services, and the entry of specialized providers has the potential to promote innovation. Sometimes "innovation" leads to lower operating costs through efficiencies made possible by consolidating operations into fewer facilities. However, such consolidation can greatly multiply the impact from a single or dual point of failure. While market forces may drive decisions to lower operating costs, market forces alone may be insufficient to prevent catastrophic impacts stemming from unchecked aggregation of functions into one or two locations across multiple state boundaries.

In its comments, the Boulder Regional Emergency Telephone Service Authority (BRETSA) points out that

[54] *See* Letter from Stacy Hartman, CenturyLink -Director Public Policy, to John Healy and Michael Connelly, Public Safety and Homeland Security Bureau, FCC (dated Jun. 12, 2014).

[55] *Derecho Report* at 43-45.

> [t]o the extent states or regional authorities may contract with 9-1-1 or NG911 providers for service, the magnitude and cost of terminating 9-1-1 service agreements, selecting a new provider (from among the few qualified) and deploying/coordinating the transition to a replacement 9-1-1 system and network, and limited public resources, and the small number of customer-PSAPs and the relatively small number of 9-1-1 calls over which those expenses may be spread, vitiates the market impacts of failures [such as the multistate outage].[56]

In other words, market forces alone are not likely to provide sufficient incentive to preserve or improve service availability, in part because the costs of transitioning to other service providers are so high.

4.2 Transition to NG911 System Architecture

The record evidence leads to the conclusion that Intrado's network architecture did not include sufficient safeguards to prevent the April multistate outage. The outage underscores the importance of incorporating such basic safeguards in the initial design of the network. Some of the states affected by this outage were dependent on Intrado's underlying NG911 architecture for 911 call completion by virtue of CenturyLink's contract with Intrado. The silent failure of the Intrado PTM, which keeps track of legacy 911 trunks in the NG911 transition architecture, did not result in an automatic failover to the backup system. The mechanism was not able to recognize that there was a problem and automatically fail over to the Miami ECMC. As the Washington State E9-1-1 Coordination Office states, the event demonstrated that active redundancy did not exist in this transitional network.[57] Further,

> [t]he outage revealed that the generation of critical alarms in response to failures along the call processing path is incomplete [and] a critical sub-system routine failed to allow call processing to continue beyond this sub-system. Because the process performed by this sub-system failed, the call ceased to be processed but no critical alarm or notification was generated to alert the NOC that a call that had entered the ECMC never completed processing through the ECMC. Subsequently the call timed out and a failure or busy notification was returned to the caller. Had the LNG been 'notified' of the failure, it could have attempted to send the call to the other router.[58]

The solution to restoring this NG911 system entailed a manual failover once Intrado identified the problem.[59]

[56] *Ex Parte* Comments of Boulder Regional Emergency Telephone Service Authority (BRETSA) at 3 (filed Jul 8, 2014) (BRETSA *Ex Parte* Comments).

[57] Washington State E9-1-1 Coordination Office at 5.

[58] *Id.* at 5

[59] The Bureau notes that the optimal solution would have been an automatic failover.

4.3 Concentration of 911 Assets

The outage also raises issues regarding reliance on geographically dispersed IPSRs. As indicated by Intrado, the "lack of ingress trunk diversity across Legacy Network Gateways (LNGs) and lack of distribution to core processing sites contributed to the outage."[60] Intrado states that, "[f]or any geographic area, originating service providers (OSPs) are in the best position to understand their serving area and to make determinations of where calls are delivered in order to achieve diversity. The nature of legacy TDM circuits to an ESInet requires cooperation and shared responsibility between the OSP and the ESInet provider in order to achieve architectural resiliency and mitigate the impact to any one geographic area (and the 9-1-1 callers within that area)."[61] 911 service providers in the NG911 environment should distribute capabilities broadly across their operational fabric to maximize availability for NG911 architectures.

4.4 Communications Among 911 Ecosystem Participants

The Bureau's investigation reveals the lack of clear lines of communication between CenturyLink's and Intrado's NOCs, between CenturyLink and PSAPs, and between Intrado and PSAPs. NG911 systems may enable efficient monitoring of critical 911 system components, regardless of what entity "owns" them. All entities in the chain of end-to-end 911 service must give serious consideration to ensuring that information about alarms associated with critical physical and logical functionalities is shared among such entities along the 911 call chain.[62]

Similarly, the investigation raises concerns that, despite the Commission's decade-long requirement that providers notify PSAPs "as soon as possible" of significant outages that potentially affect 911 service with "all available information,"[63] service providers may not have sufficient methods in place to clearly and accurately relay information expeditiously to PSAPs affected by an outage. The Bureau does not have enough information based on this inquiry to conclude that the widespread practice of direct 911 service providers – typically, ILECs – subcontracting parts of that responsibility to other providers is a universal problem. The record is clear, however, that such practice was a problem in this case. CenturyLink, a multi-function communications service provider covering a relatively large service area and with a direct relationship with Intrado, was in the best position to evaluate and monitor acceptable risk from a third-party 911 service.

Despite the fact that Intrado owned and operated the software at fault, Intrado suggests that it is not responsible for presenting a coherent picture of what happened on April 9-10, 2014.[64] Instead,

[60] Intrado Reply Comments at 6.

[61] *See* Intrado Reply Comments at 6.

[62] As noted Section 2.1 *supra*, and in apparent contradistinction to CenturyLink and Intrado, the Bureau notes that the coordination and open communication between Comcast and TCS here enabled them to reroute Comcast traffic, resulting in seamless and uninterrupted 911 call delivery.

[63] *See* 47 C.F.R. §4.9.

[64] *See* Intrado Reply Comments at 8 ("[u]nder the current circumstances, it would be improper for Intrado 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").

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."[65] It further states that, "[u]nder the circumstance, it would be improper for Intrado 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," but it is "willing to engage in a discussion of the issue."[66] "The larger Intrado enterprise may have in its possession (on behalf of its various customers) a wide range of information that might relate to a 911 outage (with its use strictly controlled by contract), and this arrangement should not be usurped or translated to an expectation or requirement that the larger Intrado enterprise must breach some of its customer contracts in order to disseminate that information in a collective, assimilated fashion."[67]

BRETSA argues otherwise: "If 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. Such rules should, of course, appropriately limit provider and PSAP or agency use of confidential and proprietary information."[68]

These comments raise the concerning potential that new business relationships emerging among 911 ecosystem participants, including third-party vendors that provide certain specialized 911 services, might have the effect of limiting or confusing lines of communication and accountability, either during an event itself, or afterwards during an investigation. While innovation can certainly have positive effects, it cannot be at the cost of facilitating an outage at a single or dual point of failure. To ensure that these failures rarely occur requires appropriate redundancy and adequate safeguards to detect failures and switch to redundant equipment.

4.5 Technology Trends that May Result in More-Widespread Outages

The April 911 outage was broad in scope, covering all PSAPs in Washington for which Englewood is the primary IPSR, along with other PSAPs directly or indirectly served by Intrado. This experience, when coupled with others, raises larger concerns about the reliability of VoIP networks generally.

Based on its review and analysis of NORS data submitted since interconnected VoIP service became subject to Part 4 of the Commission's rules, the Bureau believes large-scale outages – larger than what typically occurs with the circuit-switched PSTN – may result when VoIP networks do not

[65] *See* Intrado Reply Comments at 8.

[66] *Id.*

[67] Intrado Reply Comments at 8-9.

[68] BRETSA *Ex Parte* Comments at 2-3.

include appropriate network architectural safeguards.[69] For example, VoIP service providers may rely on one or two pieces of equipment to perform critical functions, creating the potential for a single point of failure. If these one or two pieces of equipment fail, all VoIP services for every customer for that company can be lost. The underlying IP architecture is very reliable, but the service running over that architecture may be susceptible to the failure of one or two pieces of equipment. In this regard, the NG911 transition architecture used by CenturyLink and Intrado provides insight into certain IP-supported network vulnerabilities that must be addressed going forward, for both the period of time when 911 architecture is in a transitional phase from E911 to NG911 and for true NG911.

In the existing circuit-switched PSTN, call control, including call set-up, is primarily performed in central office switches that are geographically close to the customers being served. Even failure of a large central office switch will only affect up to a few hundred thousand customers in the vicinity of the switch. This differs from VoIP, where call control can be geographically separated, far from the sites through which the callers' encoded voice signals pass. VoIP permits the call control function to be distributed among just a few large servers nationwide, each of which can serve millions, or even tens of millions, of customers. While there are benefits to this innovation, it must be implemented and executed in such a way as to account for legitimate public safety concerns.

The decision to consolidate call management functions is one made by carriers and/or PSAPs. There are a number of potential benefits to this kind of innovation. For example, it appears to be driven primarily by efficiency goals (*i.e.,* fewer nodes, less staff, lower operational expenses); in a competitive environment, consolidation holds the potential ultimately to lower costs to consumers. It also has a positive cyber defense value in that the "attack surface" for IP call management functions is reduced. At the same time, consolidation that is implemented without adequate concern for potential pitfalls has the potential to vastly expand the potential impact of network failures in comparison to what is typical for circuit switched based networks.

In addition, there are other functions of IP communications, like registration services, that are frequently concentrated in just a few servers, with each serving many customers that may be fairly geographically remote from the server location, often creating interdependencies that cross state lines. VoIP services may require that the customer device register with the network before a call is permitted, and registration servers may check with accounting servers before permitting a customer to register.[70] Call control, registration, and other functions are frequently provided redundantly, with backup systems that can handle over one hundred percent of the typical offered load; but that redundancy does not always prevent service disruptions. The problem is that, in the wake of a major outage, large numbers of people whose calls have been blocked by the network will attempt to re-register and/or call again. As described in examples below, these retries can result in demand far exceeding one hundred percent of the normal, or even peak, hour load. The excessive demand can

[69] *See also* [Page 21 and n. 66 *infra*], noting that the problems with the scale of the April 911 outage do not appear to be unique, but instead appear to a characteristic of VoIP service in general and, now, to critical 911 services.

[70] This is not exclusively an IP issue. Wireless networks use Home Location Registers (HLRs) and other systems that may serve large numbers (millions) of customers.

overload systems and produce very large outages, essentially self-inducing a distributed denial of service.

These factors have contributed to several very large outages in IP-supported services and networks, including:

- The worldwide Skype outage of December 2010. It lasted approximately 24 hours.[71]

- The AT&T U-verse voice, data, and video outage of January 2013 affecting the Southeastern and Southwestern US. This outage was reported publicly and it affected 34 markets.[72]

- Two nationwide U-verse outages in May 2010. These occurred on May 16 and May 25, 2010.[73]

These problems appear to be potential vulnerabilities of VoIP service in general and, now, to critical 911 services.[74]

4.6 Accountability in a Transitional Environment

The increased innovation and enhanced competition occurring in the 911 ecosystem have a tremendous potential to enhance the functionality and utility of 911. As commenters point out, however, these transitions must be managed in a manner that, at the very least, safeguards, and preferably improves, the current reliability of 911.[75] The multistate outage demonstrates the need for vigilant oversight of how public safety and service providers manage the deployment of NG911 systems, particularly during the transition period when legacy systems are evolving to all-IP-supported systems.

State authorities, with the Commission, clearly have an important role to play in the evolving 911 ecosystem. WUTC addressed this issue in its comments. In Washington, the WUTC has jurisdiction over the rates, services, facilities, and practices of telecommunications companies operating within the state of Washington.[76] WUTC states that, though it deregulated as competitive

[71] "CIO update: Post-mortem on the Skype outage", available online on August 12, 2013, at http://blogs.skype.com/2010/12/29/cio-update/.

[72] *See, e.g.*, "AT&T Suffering Major U-Verse Outage, Users Unable to Use TV, Voice or Internet Services," available online on August 12, 2013, at http://www.dslreports.com/shownews/ATT-UVerse-Suffering-Large-National-Outage-122841?utm_source=dlvr.it&utm_medium=twitter ; and "AT&T U-Verse Users Experience Outage," available online on August 12, 2013, at http://www.pcmag.com/article2/0,2817,2414618,00.asp.

[73] "AT&T Suffering National U-Verse Voice Outage", available online on August 12, 2013, at http://www.dslreports.com/shownews/ATT-Suffering-National-UVerse-Voice-Outage-108578.

[74] Failure of a caller's VoIP service can prevent a caller from making any calls, including 911 calls. Thus, failure of business and residential VoIP services can also prevent completion (and even initiation) of 911 calls.

[75] *See, e.g.*, BRETSA *Ex Parte* Comments at 3; Thurston 9-1-1 Communications Comments at 2.

[76] WUTC Reply Comments at 2 and n.4, *citing* Washington Revised Code§ 80.01.040 ("[t]he utilities and transportation commission shall: . . . (3) Regulate in the public interest, as provided by the public service laws, the rates, services,

many of CenturyLink's services in Washington, 911 services are not treated as competitive and therefore remain a tariffed service, subject to WUTC oversight.[77] WUTC states that it also "regulates service quality, requires reporting during major outages, regulates the E-911 obligations of local exchange companies, and mandates compliance with network performance standards that include specific requirements for E-911 facilities."[78] Under WUTC rules, each provider has the responsibility to ensure the reliability and resiliency of the portion of the 911 communications infrastructure that is under its control and ensure that it is sustained – regardless whether it subcontracts some functions to another company and regardless of the legacy or next generation nature of the underlying technology.[79]

The outage illustrates the need for 911 service providers within their respective jurisdictions to proactively address the enhanced need for reliability when implementing NG911.[80]

5. RECOMMENDATIONS FOR MAINTAINING A RELIABLE END-TO-END 911 SYSTEM

This inquiry has revealed many technical and operational challenges involved in the transition to NG911. The Bureau recommends that the Commission, state governments and 911 industry participants take the following steps to preserve the reliability and integrity of the 911 system throughout this transition and beyond.

- **Develop and Implement NG911 Transition Best Practices**: The transition to NG911 introduces new technologies, service arrangements and business relationships into the 911 ecosystem, adding complexity that heightens the risk of a widespread outage with the potential to affect multiple states. The Bureau's inquiry has shed light on a number of measures that providers can take to improve service reliability during this transition. The Bureau recommends that the Commission charge CSRIC with developing and refining a comprehensive set of best practices in this area.

- **Further FCC Proceedings on 911 Reliability:** The Commission should conduct further proceedings as necessary to ensure that reliability of 911 service in the United States continues to promote the safety of life and property by maintaining pace with evolving technologies and challenges, and that both incumbent 911 service providers and new entrants remain fully accountable to the public they serve.

facilities, and practices of all persons engaging within this state in the business of supplying any utility service or commodity to the public for compensation").

[77] WUTC Reply Comments at 2.

[78] WUTC Reply Comments at 2. These requirements do not reference the reliability or resiliency of any equipment in the 911 network.

[79] *See generally* Washington Administrative Code chapter 480-120 WAC.

[80] *See* BRETSA *Ex Parte* Comments at 4 ("Industry oversight must extend from the originating service provider and equipment manufacturers, to the third party providers which aggregate and transport 9-1-1 calls and to which originating service providers outsource their 9-1-1 compliance, to the providers which aggregate the calls within each state or region and route them to the appropriate PSAPs, and provider of all component services essential to reliable 9-1-1 Service.").

- **Intergovernmental and Stakeholder Information Sharing:** The transition to NG911 creates a need for closer coordination of evolving practices and expectations regarding 911 among all governmental and commercial entities, as well as a broad-based understanding among all stakeholders regarding the status of deployment of NG911 from all stakeholders involved.

- **Situational Awareness**: All parties involved in 911 end-to-end call completion, as well as appropriate public safety authorities, need to take steps to improve situational awareness during an outage.

- **Exercise of Enforcement Powers:** The Commission should use enforcement action as necessary to safeguard reliable end-to-end 911 service. 911 service providers must remain vigilant and ensure compliance with the Commission's 911 requirements, including outage reporting requirements, particularly as they transition to NG911 networks.

- **Contractual Relationship Monitoring**: Primary 911 service providers should monitor their contractual relationships to establish clear operational roles and responsibilities for situational awareness and information sharing, and exercise operational oversight with respect to their subcontractors and implement the appropriate mechanisms to retain meaningful controls.

6. CONCLUSION

The April 2014 multistate outage was far more than a simple software error on an otherwise uneventful spring evening in Englewood, Colorado. It was a vivid example of the vulnerabilities that IP-supported architectures may present, without sufficient network safeguards and clear lines of accountability. The issues raised in the outage go to the heart of providing reliable 911 service. Regardless of what party implements a particular component of 911 service, there must be network reliability and clear accountability from call placement to call completion.

As the Nation transitions to new methods of communications, we need to take care to ensure that our inherent trust in the 911 system does not get lost in that transition.

Public release of this *Report and Recommendations* concludes and closes Public Safety Docket No. 14-72 and PSHSB Case File Nos. 14-CCR-0001-0007.

Appendix A: Public Safety Answering Points Affected By the April 2014 Multistate Outage

State	County	County Pop.	PSAP Name	Provider
CA	BUTTE	222090	Butte County Sheriff's Department	Verizon
CA	BUTTE		Chico Police Department	Verizon
CA	BUTTE		CHP-Chico CC-Chico	Verizon
CA	BUTTE		Paradise Police Department	Verizon
CA	COLUSA	21358	Colusa County Sheriff	Verizon
CA	LASSEN	32,163	CHP-Susanville CC-Quincy	Verizon
CA	PLUMAS	18,859	Plumas County Sheriff's Department	Verizon
CA	SHASTA	178,980	CHP-Redding CC-Red Bluff	Verizon
CA	SHASTA		CHP-Redding CC-Redding	Verizon
CA	SHASTA		Shascom	Verizon
CA	SISKIYOU	43,799	Yreka Police Department	Verizon
CA	SUTTER	95,350	Yuba City Police Department	Verizon
CA	YUBA	73,340	Marysville Police Department	Verizon
FL	LEVY	39,644	Levy County Sheriff	Intrado
FL	MARTIN	151,263	Martin County Sheriff	Intrado
FL	ST. LUCIE	286,832	St Lucie County/ Sheriff Office	Intrado
MN	ANOKA	339,534	Anoka County	CenturyLink
MN	DAKOTA	408,509	Dakota Comm Center - Zone 2	CenturyLink
MN	HENNEPIN	1,198,778	Edina	CenturyLink
MN	HENNEPIN		Hennepin County	CenturyLink
MN	HENNEPIN		Minneapolis Emergency Communications	CenturyLink
MN	RAMSEY	526,714	Ramsey County	CenturyLink
MN	RAMSEY		State Patrol/Roseville	CenturyLink
MN	SCOTT	137,232	Scott County Sheriff's Office	CenturyLink
MN	WASHINGTON	246,603	Washington County	CenturyLink
NC	BRUNSWICK	115,301	Brunswick Emergency Services	CenturyLink
NC	STANLY	60,635	Stanly County	CenturyLink

PA	DELAWARE	561,973	Delaware County Emergency Communications Center	Intrado
SC	YORK	239,363	York County	Intrado
WA	ADAMS	19,067	Adams	CenturyLink
WA	BENTON	184,486	Benton County – SECOMM	CenturyLink
WA	CHELAN	73,967	Chelan/Douglas (Rivercom)	CenturyLink
WA	CLALLAM	72,312	Pencom-Clallam County	CenturyLink
WA	CLARK	443,817	Clark Regional Emergency Services Agency	CenturyLink
WA	COLUMBIA	4,032	Columbia County Sheriff's Office	CenturyLink
WA	COWLITZ	101,860	Cowlitz County 9-1-1 Center	CenturyLink
WA	FERRY	7,646	Ferry County E9-1-1	CenturyLink
WA	FRANKLIN	86,638	Franklin County Sheriff's Office	CenturyLink
WA	GARFIELD	2,256	Garfield County Sheriff's Office	CenturyLink
WA	GRANT	91,878	Multi Agency Communications Center	CenturyLink
WA	GRAYS HARBOR	71,078	Grays Harbor Communications	CenturyLink
WA	ISLAND	78,801	Island County Emergency Services Communications Center	CenturyLink
WA	JEFFERSON	30,076	JEFFCOM 9-1-1 Communications	CenturyLink
WA	KING	2,044,449	King Co Sheriff	CenturyLink
WA	KING		King Co-Bothell	CenturyLink
WA	KING		King Co-Enumclaw PD	CenturyLink
WA	KING		King Co-Issaquah PD	CenturyLink
WA	KING		King Co-Port of STTL	CenturyLink
WA	KING		King Co-Redmond PD	CenturyLink
WA	KING		King Co-Seattle PD	CenturyLink
WA	KING		King Co-Univ. of WA	CenturyLink
WA	KING		King Co-Valley Comm.	CenturyLink
WA	KING		NORCOM-King County	CenturyLink
WA	KING		Washington State Patrol-King County	CenturyLink
WA	KITSAP	253,968	Kitsap County-CENCOM	CenturyLink
WA	KITTITAS	41,765	KITTCOM	CenturyLink
WA	KLICKITAT	20,866	Klickitat County Emergency Management	CenturyLink
WA	LEWIS	75,081	Lewis County 9-1-1 Communications Division	CenturyLink
WA	LINCOLN	10,301	Lincoln	CenturyLink
WA	MASON	60,497	MACECOM	CenturyLink
WA	OKANOGAN	41,193	Okanogan County Sheriff's Office	CenturyLink

WA	PACIFIC	20,498	Pacific County Communications	CenturyLink
WA	PEND OREILLE	12,896	Pend Oreille 9-1-1	CenturyLink
WA	PIERCE	819,743	Fife Police Department	CenturyLink
WA	PIERCE		Ft Lewis/Joint Base Emer. Comm. Center	CenturyLink
WA	PIERCE		Puyallup Communications	CenturyLink
WA	PIERCE		SouthSound/LESA	CenturyLink
WA	PIERCE		Washington State Patrol-Tacoma	CenturyLink
WA	SAN JUAN	15,824	San Juan	CenturyLink
WA	SKAGIT	118,222	Skagit County 9-1-1 Emergency Communications Center	CenturyLink
WA	SKAMANIA	11274	Skamania County Sheriff's Office	CenturyLink
WA	SNOHOMISH	745,913	SNOCOM	CenturyLink
WA	SNOHOMISH		SNOPAC	CenturyLink
WA	SPOKANE	479,398	Spokane County 9-1-1 Emergency Communications	CenturyLink
WA	STEVENS	43,430	Stevens	CenturyLink
WA	THURSTON	262,388	TCOMM911	CenturyLink
WA	WAHKIAKUM	4,042	Wahkiakum County Sheriff's Office	CenturyLink
WA	WALLA WALLA	59,530	Walla Walla	CenturyLink
WA	WHATCOM	206,353	What-Comm. Communications Center	CenturyLink
WA	WHITMAN	46,570	Whitcom	CenturyLink
WA	YAKIMA	247,044	Yakima Public Safety Communications	CenturyLink

Appendix B: Information-Gathering Process

PSHSB developed the factual record of this investigation through various sources:

***Network Outage Reporting System*.** The Bureau received 12 NORS reports from nine service providers: one each from AT&T, AT&T Mobility (Cingular), CenturyLink, Frontier, Comcast, Intrado, TCS, and Verizon Business, and four from Verizon Wireless.[81] The data from the NORS filings indicated that the outage potentially affected 6,248,473 wireline users, 620,803 wireless users, and 1,999,664 interconnected VoIP users.[82] The Bureau contacted the NORS filers to obtain additional information. In the case of both CenturyLink and Intrado, the Bureau sent letters of inquiry and held in-person meetings.[83]

It became apparent from all sources, including Intrado and CenturyLink, that while other 911 service providers and third-party contractors were tangentially involved in the outage,[84] this was largely an issue involving Intrado's equipment failure and the effect it had on 911 callers in areas served by CenturyLink. Put simply, over 95 percent of the over 11 million people affected by the outage live in territories served by CenturyLink and, by extension, Intrado.

[81] *See* NORS Report File Nos. 14-10030864 (CenturyLink); 14-10052883 (Comcast); 14-10026025 (Frontier); 14-10040868 (Intrado); 14-10028664 (TCS); 14-10159056 (Verizon Business); 14-10032612 (Verizon Wireless); 14-10032869 (Verizon Wireless); 14-10033024 (Verizon Wireless); 14-10033534 (Verizon Wireless).

[82] The Bureau notes that, as of December 16, 2012, both facilities- and non-facilities-based interconnected VoIP providers have an obligation to detect and report outages. *See* 47 C.F.R. §4.9(g); 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, 27 FCC Rcd 2650 (2012).

We note that the number of users affected as reported by NORS filers is roughly 8.87 million (wireline, wireless, and interconnected VoIP combined), while elsewhere in this Report, we indicate that over 11 million persons were affected by the outage. The former number (8.87 million) reflects the assumption built into the NORS database of the estimated number of telephone numbers in an area served by a NORS filer, while the latter number (over 11 million) reflects the population of all the counties served by the various PSAPs that were affected by this outage.

[83] Case File Nos. PSHSB – 14 – CCR – 0001-0007. Under FCC rules, data collected pursuant to NORS are presumed confidential to protect proprietary and competitive. *See* In the Matter of New Part 4 of the Commission's Rules Concerning Disruptions to Communications, *Report and Order and Further Notice of Proposed Rule Making,* 19 FCC Rcd 16830 (2004); *see also* 47 C.F.R. §4.2. The Bureau treats follow-up data and discussions between NORS reporting companies and FCC staff as also presumptively confidential as part of the NORS process. For information derived from outage reports or other confidential sources that appears in this report, the provider has agreed to waive its claim of confidentiality. Other data may be presented in the aggregate to preserve confidential protections.

[84] The Commission defines a covered service provider as any entity that (A) provides 911, E911, or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities, directly to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as defined in sections 64.3000(b) and 20.3; and/or (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, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP. 47 C.F.R §12.4(a)(4). *See also* In the Matter of Improving 911 Reliability, *et al*., PS Docket No. 13-75 *et al*., *Report and Order*, 28 FCC Rcd 17476 (2013).

***Communications with local and state authorities*:** The Bureau interviewed officials from PSAPs in Washington, North Carolina, South Carolina, California, and Minnesota.

Bureau staff ascertained that each affected PSAP, either on its own or working with fellow PSAPs and state 911 agencies learned generally what had happened (that there was an equipment breakdown somewhere in the 911 call chain preventing delivery of 911 calls to the appropriate PSAP), and that personnel at those PSAPs were able to take alternative actions, other than re-routing 911 calls, to preserve public safety (*e.g.*, through the use of public service announcements, social media, highway message signs, and distribution of 10-digit administrative numbers).

In addition, York County, South Carolina, reported that all landline phone calls were lost. According to the PSAP, it first became aware of the outage when it called Intrado.[85] In Brunswick County, North Carolina, the PSAP was, in fact, able to transfer calls to a back-up PSAP, meaning no calls were lost.[86] Meanwhile, in Hennepin County, Minnesota, and surrounding counties, the Metropolitan Emergency Services Board (MESB) supports PSAPs for the cities of St. Paul/Minneapolis and the following counties: Anoka, Carver, Dakota, Hennepin, Isanti, Ramsey, Scott and Washington. MESB indicated that the entire MESB service area was affected missing 73 wireless 911 calls, including Hennepin County. Of these 73 calls, Ramsey County (22 calls) and Hennepin County (15 calls) were the most impacted. No wireline calls were reported lost.[87]

Bureau staff contacted the public service commissions in each affected state to determine what, if any, additional administrative activity regarding the outage was occurring at the state level. In several cases, the Bureau's call was the first time that state staff was alerted to the possibility that consumers and one or more PSAPs in that state might have been affected by the April 2014 outage.

The Washington Utilities and Transportation Commission (WUTC) initiated a formal investigation into the circumstances of the outage on April 10, 2014.[88] On April 27, in response to the WUTC commencing the investigation and in compliance with Washington Administrative Code (WAC) 480-120-439, CenturyLink filed its Major Outage Report, providing WUTC with its explanation of how the outage occurred, how many people in Washington were affected, and how CenturyLink working with Intrado resolved the issue.[89] The WUTC intends to release its findings in Fall 2014. As of the date of this report, no other state has initiated administrative action.

[85] CCR Telephone Interview with Gary Loflin, Director, Public Safety Communications, York County (May 12, 2014).

[86] CCR Telephone Interview with Lt. Todd Coring, Brunswick County Sherriff's Office (May 12, 2014).

[87] CCR Telephone Interview with Pete Eggimann, Director of 911 Service, Minneapolis/St. Paul Metropolitan Emergency Services Board (Sep. 16, 2014). We note the discrepancy between the number of counties affected as reported by Intrado (6) and by MESB (8). As of the date of this Report, Intrado has indicated that it continues to work with MESB on resolving this issue (*i.e.*, whether the Counties of Carver and Isanti were or were not affected), and why only wireless calls appear to have been affected.

[88] *See* "State regulators to investigate [April 10, 2014] statewide 911 service outage," Washington Utilities and Transportation Commission, Docket No. UT-140597, available at http://www.utc.wa.gov/docs/Pages/DocketLookup.aspx?FilingID=140597 (accessed Aug. 6, 2014).

[89] *See* Letter from Mark S. Reynolds, Northwest Region Vice President, Public Policy, CenturyLink, to Steven V. King, Executive Director and Secretary, WUTC (dated Apr. 27, 2014), available at

Public Safety and Homeland Security Bureau Public Notice. On May 16, 2014, the Bureau released a Public Notice seeking comment on the effects of the outage.[90] In response, the Bureau received five comments and four reply comments.

CenturyLink wrote of the actions that it, working with Intrado, took to resolve the issue and prevent its reoccurrence.[91] TIA urged that the Commission "should refrain from taking regulatory action and encourage and allow network operators and vendors to continue their voluntary efforts in improving the reliability of their networks."[92] Intrado cautioned that the Federal policy of "encourag[ing] innovation in the development and deployment of [ ] NG 911 network . . . would be dramatically frustrated if U.S. citizens had to wait for the benefits of innovation until technology could be deployed without a flaw or the possibility of a flaw" and noted that any Commission message "should be sensitive to the chilling effect that unfair punitive measures could have on future innovation and cutting-edge deployments that save American lives and property."[93]

The King County (WA) E911 Program Office provided a nine-point list of items it sought to bring to the Commission's attention. It argued that neither CenturyLink nor Intrado provided any instructions to PSAPs on what they could do to mitigate the outage. It also noted that there is significant lack of load balancing among 911 trunk calls to the four Legacy Network Gateways (LNGs) that serve Washington; and that once Intrado realized that there was a problem, they had to call in technicians and engineers from home to identify the cause and scope of the problem, which delayed the rerouting of 911 calls by several hours.[94]

http://www.utc.wa.gov/_layouts/CasesPublicWebsite/GetDocument.ashx?docID=6&year=2014&docketNumber=140597.

[90] *See* Public Safety and Homeland Security Bureau Announces Inquiry Into Circumstances of Major 911 Outage Centered in Washington State On April 9-10, 2014, *Public Notice*, 29 FCC Rcd 5327, PS Docket No. 14-72 (PSHSB May 16, 2014) ("Multistate Outage Public Notice").

[91] *See generally* Comments of CenturyLink ("CenturyLink Comments"). We note that CenturyLink submitted confidential comments, and comments intended for public viewing, into the Commission's Electronic Comment Filing System (ECFS). The observations we make here regarding CenturyLink's comments are solely from its publicly-viewable comments.

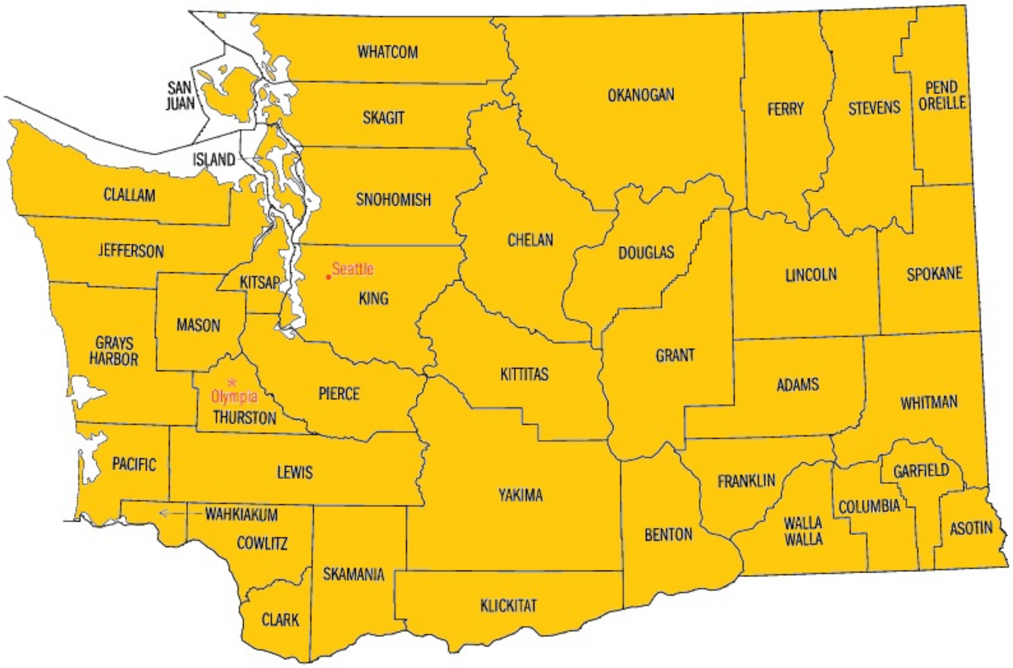
[92] *See* Comments of the Telecommunications Industry Association ("TIA Comments") at 8 (filed Jun. 16, 2014).

[93] *See* Reply Comments of Intrado ("Intrado Reply Comments") at 8-9 (filed Jun. 30, 2014).

[94] *See* Comments of King County at 1-3 (filed Jun. 15, 2014) The Washington State E9-1-1 Coordination Office's reply comments generally supported and reiterated King County's comments. *See* Washington E911 Coordinator Reply Comments. The Pacific County Sheriff's Office expressed concern over the lack of communications during the outage. *See* Pacific County Sheriff's Comments at 1.

Appendix C: States and Counties (With Combined County Populations) Affected

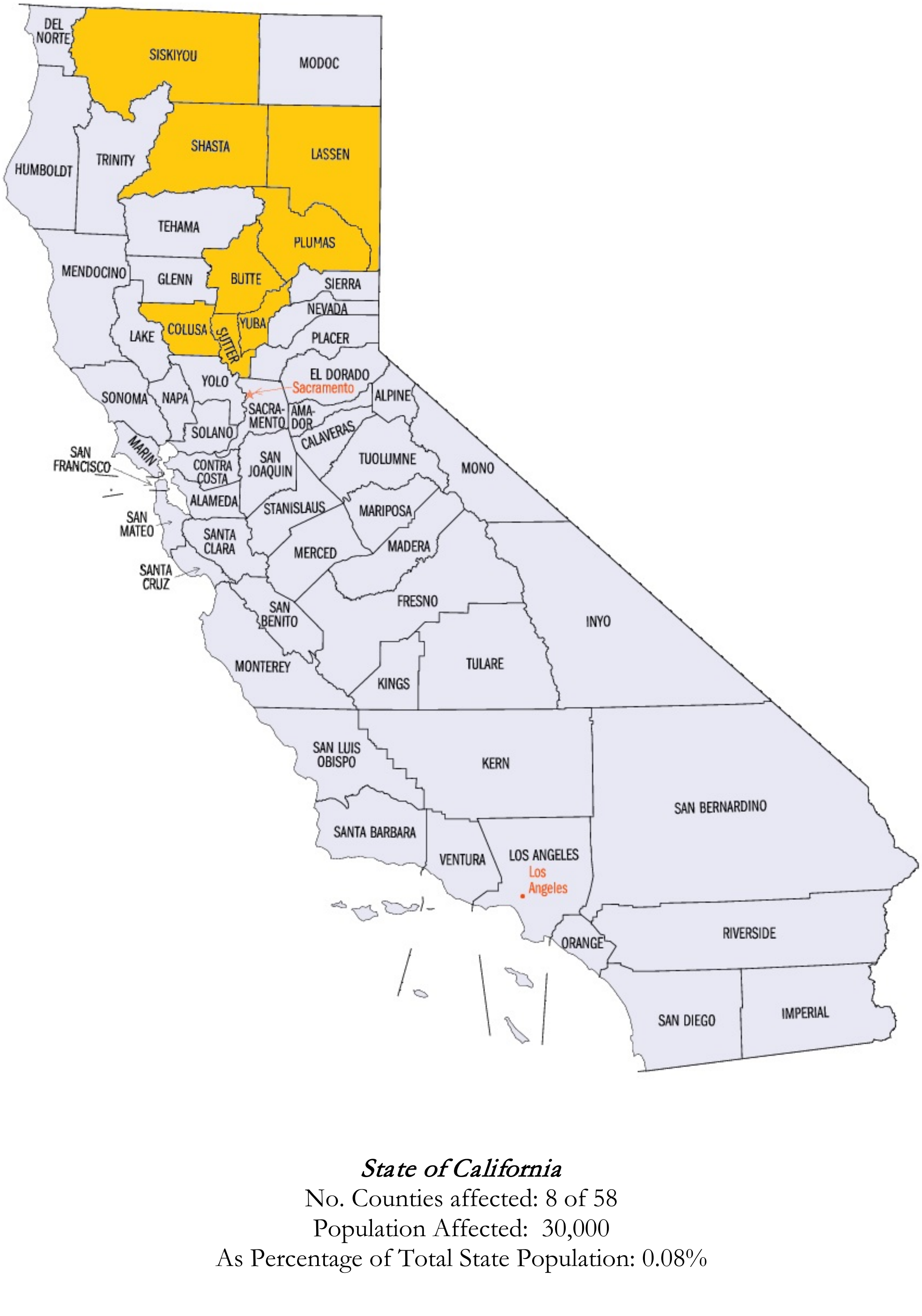
The outage at Intrado's Englewood ECMC affected eighty-one PSAPs in seven states, with the majority of the effect in Washington State, in terms of population, area, and number of PSAPs affected:[95]



State of Washington
No. Counties affected: 39 of 39
Population Affected: 6,971,406[96]
As Percentage of Total State Population: 100%

[95] *See* E-Mail from Craig W. Donaldson, Senior Vice President, Regulatory, Government & External Affairs, Regulatory Counsel, Intrado (Jul. 10, 2014). Maps and population estimates (2013) from United States Census Bureau, "State & County QuickFacts," available at http://quickfacts.census.gov/qfd/maps/ (accessed Aug. 18, 2014) and http://quickfacts.census.gov/qfd/index.html# (population).

[96] For "Population Affected," the Bureau used 2013 estimated population figures provided by the United States Census Bureau, "State & County QuickFacts," http://quickfacts.census.gov/qfd/index.html.

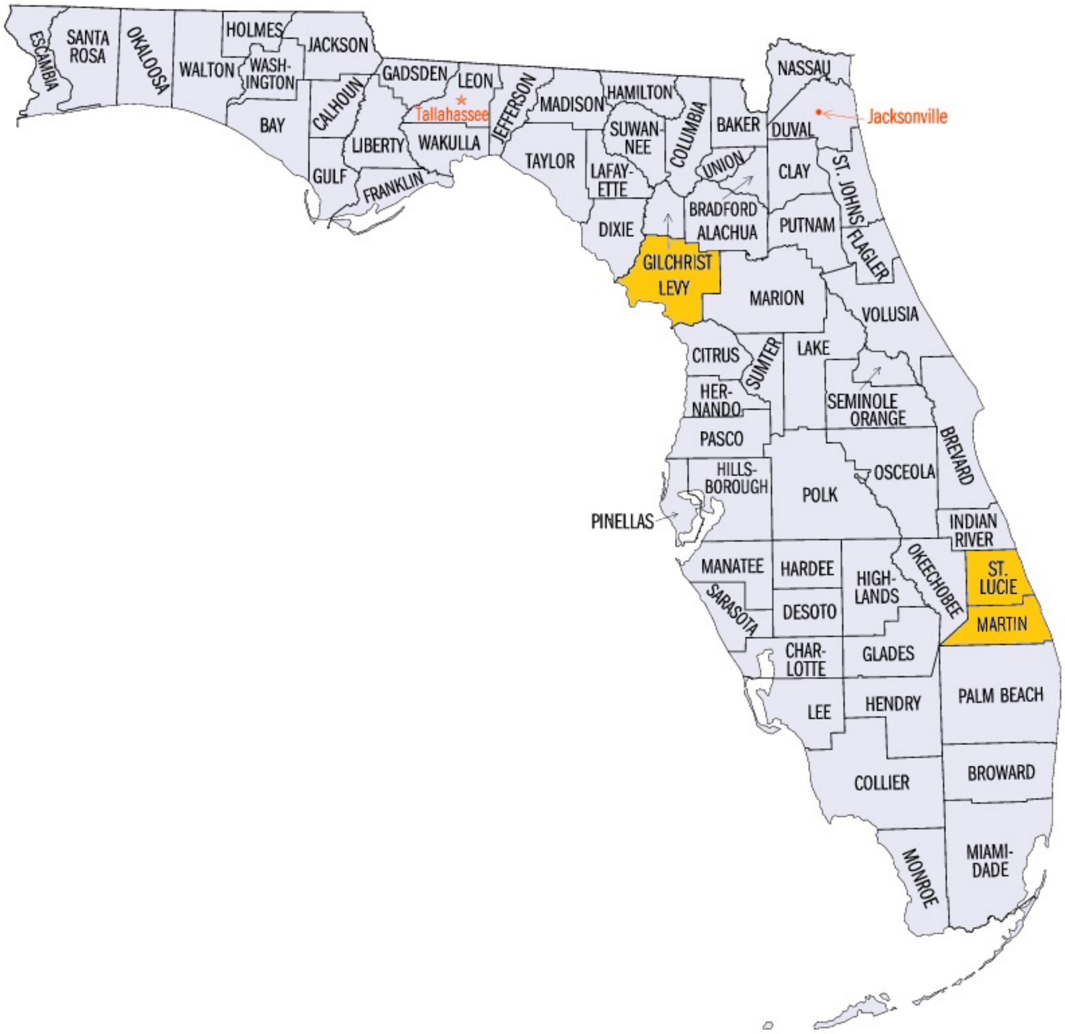


State of California

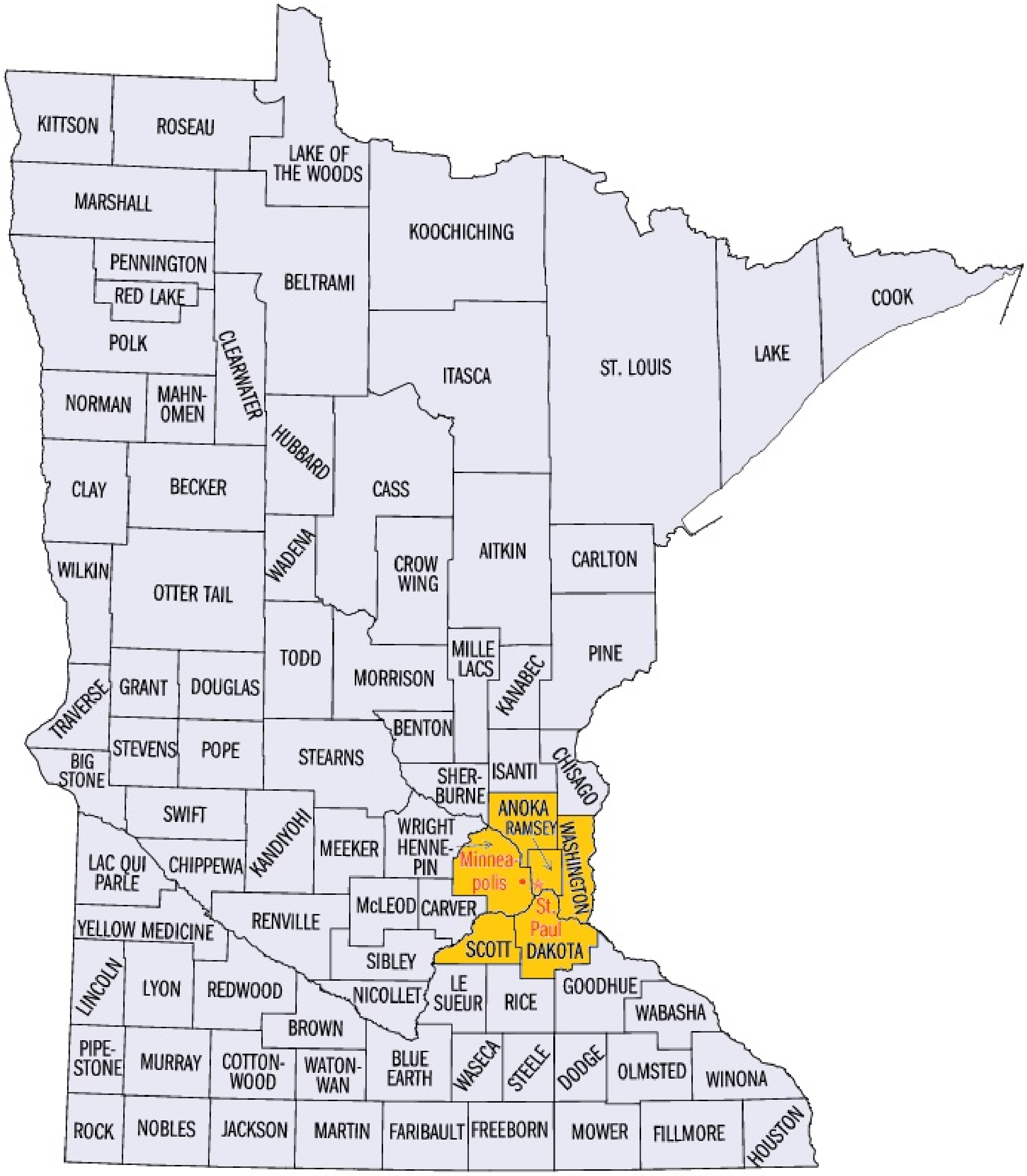
No. Counties affected: 8 of 58

Population Affected: 30,000

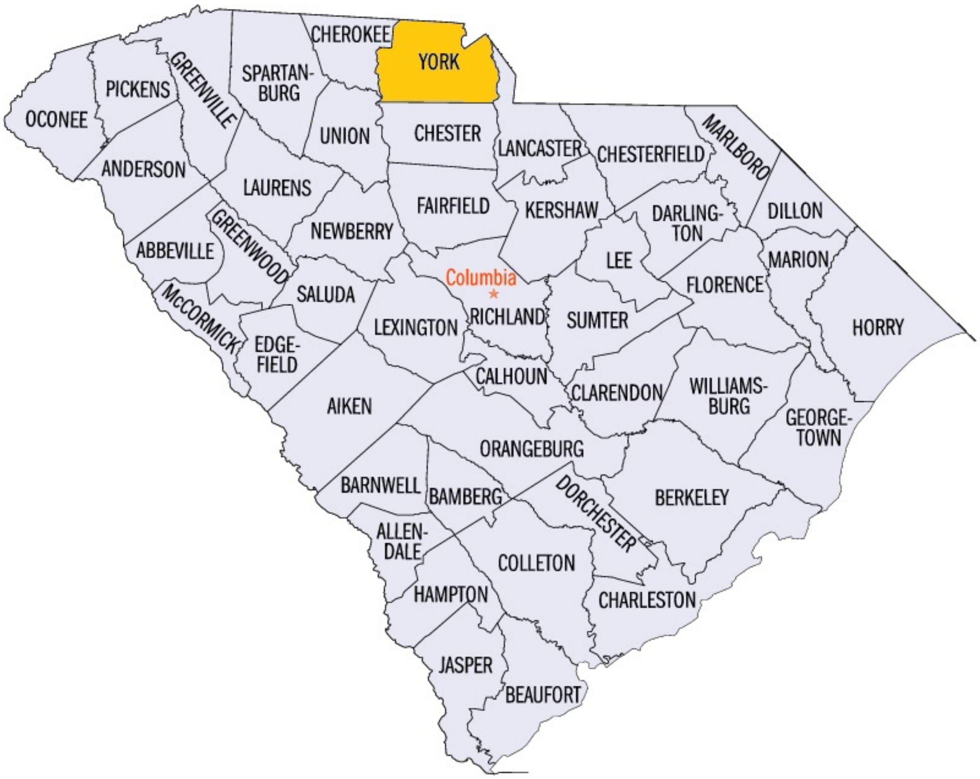
As Percentage of Total State Population: 0.08%



State of Florida
No. Counties affected: 3 of 67
Population Affected: 477,739
As Percentage of Total State Population: 2.44%



State of Minnesota
No. Counties affected: 6 of 87
Population Affected: 2,857,370
As Percentage of Total State Population: 52.72%

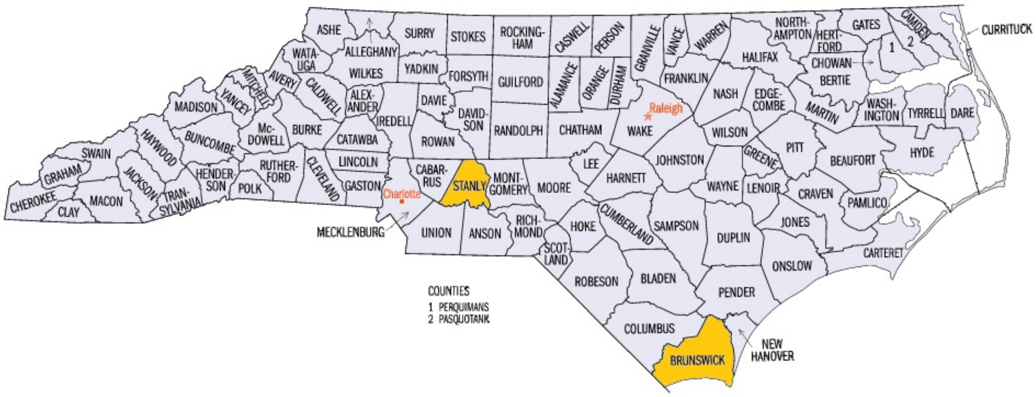


State of South Carolina

No. Counties affected: 1 of 46

Population Affected: 239,363

As Percentage of Total State Population: 5.01%

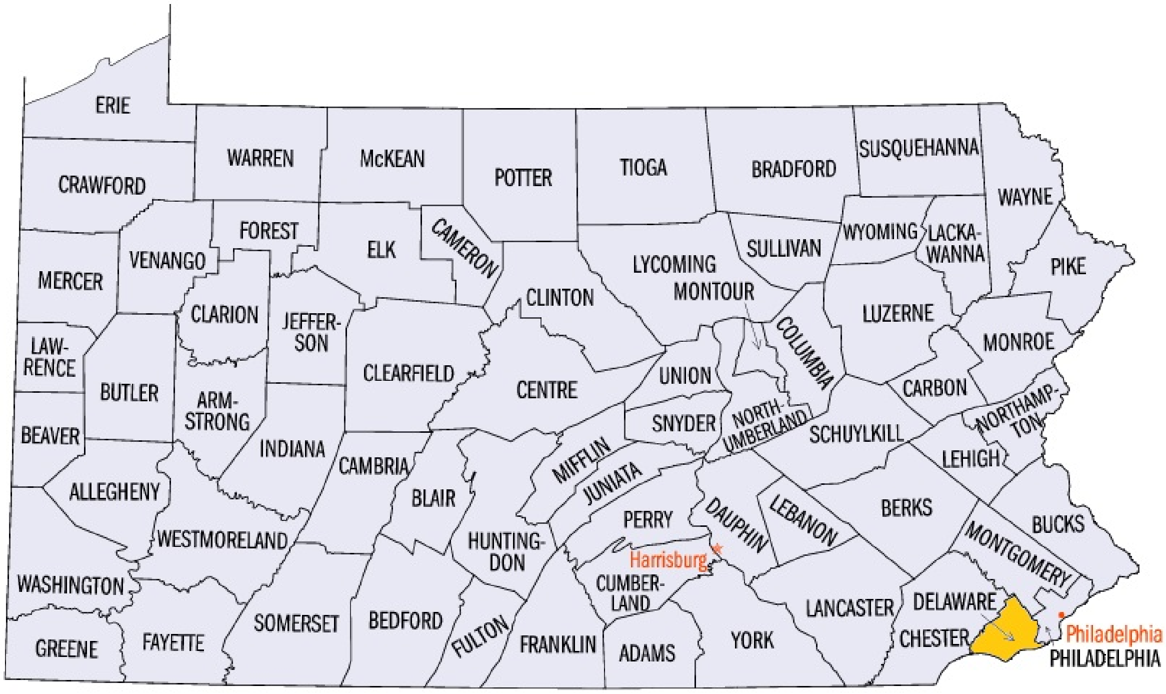


State of North Carolina

No. Counties affected: 2 of 100

Population Affected: 175,936

As Percentage of Total State Population: 1.79%



Commonwealth of Pennsylvania
No. Counties affected: 1 of 67
Population Affected: 561,973
As Percentage of Total State Population: 4.4%

Appendix D: Actions to Remedy The Outage and Prevent a Similar Occurrence (As redacted by Intrado)

Change	Date change implemented	Status
PTM counter limit for both ECMCs have been increased such that it is not possible to reach exhaustion.	4/10/2014	Completed
PTM counter value checked weekly to ensure the value is not nearing the maximum threshold.	4/10/2014	Check is occurring weekly; PTM counter value is not nearing the maximum threshold.
[redacted] alarm instructions updated to indicate severity, troubleshooting steps, and immediate escalation to technical on-call resource.	4/10/2014	Intrado NOC has been trained on updated procedures.
ECMC site failover documentation validated; staff trained on failover procedures.	4/16/2014	Completed
General [redacted] alarms reviewed and specific, actionable alarms created.	4/14/2014	Complete
Alarm created based on percentage of successful calls processed on a given ECMC compared to total calls for that ECMC over a 15 minute sample period.	4/15/2014	Complete. Alarming validated and procedures updated.
Changes completed to reroute calls on an individual basis to the other ECMC if for some unforeseen reason it cannot complete processing.	5/19/2014	Individual call failover between ECMCs completed.
Further reviews and continuous improvement underway; recommended changes will be scheduled as appropriate	No items to schedule	Ongoing – No additional modifications identified.
Work with carriers to review ingress call distribution between ECMC's; implement recommended changes		Meetings taking place [redacted] to identify appropriate network recommendations.
Additionally, to prevent possible	Scheduled for end of	Memory management

recurrence of reaching PTM counter limit, moving from using database insertion technique to memory management approach.	year 2014	approach development underway; This change is not necessary to mitigate the possibility of another outage. Other corrective actions have done so.