

**Exh. JDW-1CT
Docket UT-181051
Witness: James D. Webber
REDACTED VERSION**

**BEFORE THE WASHINGTON
UTILITIES AND TRANSPORTATION COMMISSION**

**WASHINGTON UTILITIES AND
TRANSPORTATION COMMISSION,**

Complainant,

v.

**CENTURYLINK
COMMUNICATIONS, LLC,**

Respondent.

DOCKET UT-181051

**TESTIMONY OF
JAMES D. WEBBER
ON BEHALF OF
STAFF OF THE
WASHINGTON UTILITIES AND
TRANSPORTATION COMMISSION**

December 15, 2021

**CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET UT-181051
REDACTED VERSION**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35

CONTENTS

I. INTRODUCTION..... 1
II. SCOPE AND SUMMARY OF TESTIMONY 4
III. THE WASHINGTON STATE E911 SYSTEM AND ITS CRITICAL IMPORTANCE
FOR PUBLIC SAFETY 8
IV. THE CAUSE OF THE DECEMBER 27-29, 2018 OUTAGE..... 17
V. IDENTIFICATION OF CIRCUITS IMPACTED BY THE CENTURYLINK OUTAGE
34
VI. ANALYSIS OF 911 CALLING DATA DURING THE OUTAGE PERIOD 44

LIST OF FIGURES

Figure 1: Representative Next Generation 911 System..... 12
Figure 2: Infinera Switching Nodes and Line Modules..... 20
Figure 3: Illustration of [REDACTED]s Linking Infinera Line Modules 21
Figure 4: [REDACTED] 28
Figure 5: The Four CenturyLink Circuits Relied Upon by TSYs for SS7 Connectivity 40
Figure 6: The [REDACTED] Failure Disrupted TSYs’ Signaling and Call Processing to
PSAPs 41
Figure 7: Chart of E911 Call Counts During the December 2018 Outage 52
Figure 8: Period 2 Impacts on Calls to TSYs-Served PSAPs..... 57
Figure 9: Period 2 Impacts on Calls to CenturyLink-Served PSAPs 58
Figure 10: Failed Calls During Period 2 for [REDACTED] Served by CenturyLink.. 60

LIST OF TABLES

Table 1: Impacts of the December 2018 Outage on Washington E911 Calls 44
Table 2: E911 Call Counts, for TSYs-Served PSAPs..... 53
Table 3: E911 Call Counts, for CenturyLink-Served PSAPs 55
Table 4: Period 2 Impacts on Calls to TSYs-Served PSAPs 57
Table 5: Period 2 Impacts on Calls to CenturyLink-Served PSAPs..... 58

LIST OF EXHIBITS

1		
2		
3	Exhibit JDW-2	James D. Webber CV
4	Exhibit JDW-3C	Docket UT-181051 Staff Investigation Report Narrative
5	Exhibit JDW-4	FCC Report Narrative, August 2019
6	Exhibit JDW-5C	Attachments 3a and 3c to CenturyLink Response to Staff Data
7		Request 3(C)
8	Exhibit JDW-6C	CenturyLink Responses to Staff Data Requests (C)
9	Exhibit JDW-7	National 911 Annual Report: 2019 Data
10	Exhibit JDW-8	National 911 Progress Report: November 2019
11	Exhibit JDW-9	National Emergency Number Association Definitions
12	Exhibit JDW-10	National Emergency Number Association Next Generation 911
13		Diagram
14	Exhibit JDW-11	Washington Military Department NG911 Transition Announcement
15	Exhibit JDW-12	National Emergency Number Association 911 Origin and History
16	Exhibit JDW-13	UTC Comments to FCC, PS Dockets 14-193; 13-75
17	Exhibit JDW-14C	CenturyLink Confidential Root Cause Analysis Filed Feb. 12, 2019
18	Exhibit JDW-15	CSRIC Best Practices, July 24, 2018
19	Exhibit JDW-16	Public Safety and Homeland Security Bureau Notice DA-19-1039
20	Exhibit JDW-17	National Security Agency, Hardening Network Devices, PP-20-0702
21	Exhibit JDW-18C	CenturyLink Responses to Public Counsel Data Requests
22	Exhibit JDW-19C	TSYS Responses to Public Counsel Data Requests
23	Exhibit JDW-20C	Attachment B.1(b) to TSYS Response to PC Data Request 4
24	Exhibit JDW-21C	Attachment 2 to TSYS Response to PC Data Request 23
25	Exhibit JDW-22C	TSYS Response to Staff Data Request 3 and Attachments
26	Exhibit JDW-23C	TSYS Response to Staff Investigation Data Requests
27	Exhibit JDW-24	CenturyLink Responses to Consumer Protection Investigation Data
28		Requests
29	Exhibit JDW-25	CenturyLink Responses to Staff Investigation Data Requests RS-1 –
30		RS-11, September 2019
31	Exhibit JDW-26C	Attachments A and B to CenturyLink Response to RS-7 and RS-8

- 1 Exhibit JDW-27C CenturyLink Response to Staff Investigation Data Request October 2,
- 2 2020
- 3 Exhibit JDW-28C Attachment 1 to CenturyLink Response October 2, 2020
- 4 Exhibit JDW-29C CenturyLink Response to Staff Investigation Data Request September
- 5 18, 2020
- 6 Exhibit JDW-30C Attachment 2 to CenturyLink Response September 18, 2020
- 7 Exhibit JDW-31C Attachment to CenturyLink Response to Staff Data Request 20
- 8 Exhibit JDW-32C TSYS Major Outage Report January 14, 2019

1 **I. INTRODUCTION**

2

3 **Q. Please state your name and business address.**

4 A. My name is James D. Webber. My business address is 4240 Colton Circle,
5 Naperville, Illinois 60564.

6

7 **Q. By whom are you employed and in what capacity?**

8 A. I am a Partner and Senior Vice President at QSI Consulting, Inc. (“QSI”).

9

10 **Q. How long have you been employed by QSI?**

11 A. Eighteen years. I joined the firm in 2003 as a Senior Consultant and became a
12 Partner and Senior Vice President 2007.

13

14 **Q. Would you please state your educational and professional background?**

15 A. I earned a Bachelor of Science in Economics and Business Administration in 1990,
16 and a Master of Science in Economics in 1993, both from Illinois State University. I
17 have nearly 30 years of experience in the regulated utilities industry, with most of
18 my time focused on competitive and technical issues in the telecommunications
19 sector. As discussed below, I previously worked as a State Public Utility
20 Commission (“PUC”) staff analyst and manager. My professional experience
21 includes consulting for numerous companies in the communications sector, working
22 for both large and small communications services providers and, as outlined in my

1 CV, co-founding and managing an enhanced service provider, and serving as a
2 member-manager of a developing Competitive Local Exchange Carrier (“CLEC”).¹

3 I have experience testifying before the Federal Communications Commission
4 (“FCC”), PUCs, arbitrators, and state and federal courts throughout the United States
5 on a wide variety of topics, including telecommunications business processes and
6 practices, cost methodologies, economic damages, interconnection, pricing, and
7 public policy, among others.

8 Prior to joining QSI in 2003, I worked for ATX/CoreComm as the Director
9 of External Affairs. In that capacity, my responsibilities included: management and
10 negotiation of interconnection agreements and other contracts with other
11 telecommunications carriers; management and resolution of operational impediments
12 arising from relationships with other carriers (such as the unavailability of shared
13 transport for purposes of intraLATA toll traffic, or continual problems associated
14 with failed hot cut processes); management of financial disputes with other carriers;
15 design and implementation of cost minimizations initiatives; design and
16 implementation of legal and regulatory strategies; and, management of the
17 Company’s tariff and regulatory compliance filings. I also assisted in the Company’s
18 business modeling as it related to the use of Resale services, and Unbundled
19 Network Elements (“UNEs”), for example, UNE-Loops and UNE-Platform.

20 From November 1997 to October 2000, prior to joining ATX/CoreComm, I
21 held positions within AT&T’s Local Services and Access Management organization
22 and its Law and Government Affairs organization. As District Manager within the

¹ Webber, Exh. JDW-2.

1 Local Services and Access Management organization I was responsible for local
2 interconnection and billing assurance. Prior to that position, I served as a District
3 Manager – Law and Government Affairs, where I implemented AT&T’s policy
4 initiatives at the state level.

5 Prior to joining AT&T, I worked (July 1996 to November 1997) as a Senior
6 Consultant with Competitive Strategies Group, Ltd. (“CSG”), a Chicago-based
7 consulting firm that specialized in competitive issues in the telecommunications
8 industry. While working for CSG, I provided expert consulting services to a diverse
9 group of clients, including telecommunications carriers and financial services firms.

10 From 1994 to 1996, I worked for the Illinois Commerce Commission (“ICC”)
11 where I served as an Economic Analyst and, ultimately, as manager of the
12 Telecommunications Division’s Rates Section. In addition to my supervisory
13 responsibilities, I worked closely with the ICC’s engineering department to review
14 Local Exchange Carriers’—and to a lesser extent Interexchange Carriers’ (“IXCs”)
15 and Competitive Local Exchange Carriers’—tariffed and contractual offerings as well
16 as the supporting cost, imputation, and aggregate revenue data.

17 From 1992 to 1994, I worked for the Illinois Department of Energy and
18 Natural Resources, where I modeled electricity and natural gas consumption and
19 analyzed the potential for demand side management programs to offset growth in the
20 demand for, and consumption of, energy. In addition, I analyzed policy options
21 regarding Illinois’ compliance with environmental legislation.

1 **II. SCOPE AND SUMMARY OF TESTIMONY**

2
3 **Q. Mr. Webber, have you testified previously before the Washington Utilities and**
4 **Transportation Commission (“Commission”)?**

5 A. Yes. I last testified in WUTC Docket No. UT-063061 on behalf of Eschelon
6 Telecom, Inc., and in WUTC Docket No. UT-083041 on behalf of Charter Fiber
7 Link WA-CCVII, LLC.

8
9 **Q. On whose behalf was your testimony here today prepared?**

10 A. I prepared this testimony on behalf of the Commission’s Staff (“Staff”).

11
12 **Q. Mr. Webber, can you please describe the scope of your testimony?**

13 A. This testimony presents my understanding of the causes and impacts of the major
14 service outage experienced by the Washington state Enhanced 911 (“E911”) public
15 safety communications network during December 27-29, 2018. Staff engaged my
16 firm, QSI Consulting, to follow up on Staff’s earlier investigations into this outage
17 by conducting an independent investigation and analysis of those causes and
18 impacts. Under my direction, my team and I have reviewed the relevant information
19 that Staff previously obtained and provided to us, including: its December 2020
20 Investigation Report and supporting Appendices filed in this docket;² the August
21 2019 report by the FCC’s Public Safety and Homeland Security Bureau (“PSHSB”)³
22 on the national outage experienced by CenturyLink Communications, LLC

² Webber, Exh. JDW-3C.

³ Webber, Exh. JDW-4.

1 (“CenturyLink” or “Company”)⁴ on its ██████████ long-haul fiber network coincident
2 with the Washington 911 outage; and numerous discovery requests and responses,
3 and documents produced in this proceeding by other parties, including CenturyLink,
4 TeleCommunication Systems, Inc. (“TSYS”),⁵ and the Washington Military
5 Department (“WMD”) and its State E911 Coordinator’s Office (“SECO”). QSI also
6 assisted Staff with propounding additional data requests to those parties and
7 reviewing their responses, and conducted some independent research. I considered
8 all of these materials when formulating the analyses and conclusions set forth in this
9 testimony, which are my own.

10
11 **Q. Mr. Webber, can you please summarize your testimony in this matter?**

12 A. Yes, certainly. The Washington state E911 communications system is a critical
13 component of the state’s public safety infrastructure. While behind the scenes there
14 is a highly complex telecommunications and public safety network that delivers
15 E911 service, the ordinary Washington citizen relies on the knowledge that if they or
16 a loved one is stricken with an emergency situation—e.g., a heart attack or other
17 medical emergency, a traffic accident, a fire, or some other threat to health, life or
18 property—help from appropriate emergency responders can be sent on the way by the
19 simple act of dialing “911” on their telephone.

20

⁴ On January 7, 2021, CenturyLink filed a notice with the Commission, stating that the company had adopted a new trade name, Lumen Technologies Group. *See*, Docket UT-210015.

⁵ Telecommunication Systems, Inc. is the company’s name as registered with this Commission. Comtech Telecommunications Corp. is its parent company.

1 In the early morning of December 27, 2018, Washington began undergoing a
2 CenturyLink caused, state-wide outage of its E911 system that lasted for more than
3 two days into December 29, 2018. Washington residents and businesses attempting
4 to make E911 calls during that time experienced fast busy signals, or were unable to
5 connect and many thousands of calls failed. Moreover, calls that were connectd to
6 Washington’s public safety answering points (“PSAPs”) impairments to the delivery
7 of callers’ location information, which normally helps expedite emergency
8 responses.

9 At the time of the outage, CenturyLink had been the incumbent E911 service
10 provider in Washington for several years but was in the process of transferring that
11 role to a new provider, TSYs. The Washington E911 disruption was part of a much
12 wider outage occurring at that time on one of CenturyLink’s fiber-based long-haul
13 transport networks, referred to as the [REDACTED]. The [REDACTED] outage
14 entirely disrupted or impaired many CenturyLink services in multiple states and had
15 rippling effects on other service providers relying upon that network, including 911
16 service providers in several states in addition to Washington. CenturyLink estimated
17 that its [REDACTED] outage caused over 12-million calls across the country to be
18 blocked or degraded.⁶

19 Based on the QSI investigation that I directed and participated in, I conclude
20 that the primary and avoidable cause of the Washington E911 network outage in
21 December 2018 was CenturyLink’s failure to disable certain unused communications
22 paths, known as [REDACTED], between the

⁶ Webber, Exh. JDW-4 at 8.

1 nodes on its [REDACTED]. Those “unlocked” (i.e., enabled)
2 [REDACTED] were the primary reason that just four malformed packets could propagate
3 and escalate into a debilitating packet storm that crippled the [REDACTED] across
4 dozens of states for over two days, and led to the outages experienced on
5 Washington’s E911 system.

6 What I find most striking about this circumstance is that CenturyLink had
7 suffered a highly-similar [REDACTED]

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]

19 [REDACTED]⁷ In response to
20 Staff discovery asking whether that action in fact occurred for the [REDACTED],
21 CenturyLink declined to provide a straight answer. [REDACTED]

22 [REDACTED]
23 [REDACTED]
24 [REDACTED]⁸ CenturyLink is

⁷ Webber, Exh. JDW-5C at 9.

⁸ Webber, Exh. JDW-6C.

1 ultimately responsible for managing its networks in a prudent manner, and by failing
2 to lock down the unused [REDACTED] on its [REDACTED], it likely bears direct
3 responsibility for the [REDACTED] packet storm and outage, and the ensuing
4 E911 system failures across Washington.

5 I also conclude that the primary driver of the disruptions to Washington's
6 E911 service during the outage was that four SS7 circuits, provided over
7 CenturyLink's [REDACTED], failed due to the packet storm. The failure of those
8 circuits prevented TSYS and the PSAPs it served from completing E911 calls and
9 obtaining callers' address information for several extended periods of time during
10 that two-day outage period in December 2018. I have also seen evidence that PSAPs
11 that were still being served directly by CenturyLink's network were also
12 experiencing call disruptions, but their causes are not yet clear, and that investigation
13 is ongoing.⁹ Based upon the data available to date, I estimate that the December 2018
14 outage caused nearly [REDACTED] calls made to the Washington E911 system to fail,
15 constituting nearly [REDACTED] of the total E911 call volume over that period.

16
17 **III. THE WASHINGTON STATE E911 SYSTEM AND ITS CRITICAL**
18 **IMPORTANCE FOR PUBLIC SAFETY**

19 **A. The Washington state E911 communications system is a critical**
20 **component of the state's public safety infrastructure and all participants**
21 **in that system bear a joint responsibility for ensuring its integrity and**
22 **continuous availability to the public.**

⁹ Webber, Exh. JDW-31C

1 **Q. Mr. Webber, what is the Washington state E911 communications system and**
2 **why is it so important to the welfare of the state’s residents?**

3 A. In the simplest terms, Washington’s E911 system is a statewide communications
4 system specifically designed to provide easy and rapid access to emergency services
5 first responders (e.g., police, firefighters, ambulances) by dialing a uniform 3-digit
6 code, 9-1-1. The “Enhanced” aspect is that when a 911 call is made, information
7 about the caller’s geographic location can be retrieved and transmitted in parallel to
8 that call, with both routed directly to a calling center, known as a Public Safety
9 Access Point (“PSAP”), serving the area where the call originated. At the PSAP, the
10 911 call is answered by trained personnel who assess the situation and dispatch
11 emergency services as needed. There are currently 78 PSAPs in Washington to serve
12 all of the state’s 39 counties and its population of greater than 7.7 million residents.¹⁰

13 For the ordinary citizen who is not involved in the telecommunications
14 industry or its efforts to make E911 service available, it is easy to take this system
15 for granted. For them, it is simply the knowledge that if they or a loved one is
16 stricken with an emergency situation—e.g. a heart attack or other medical emergency,
17 a traffic accident, a fire, or some other threat to health, life or property—help from
18 appropriate emergency responders can be sent on the way by the simple act of
19 dialing “911” on their telephone, smartphone, or other device. But behind the scenes,
20 there is a highly complex telecommunications system that is intended to function

¹⁰ See, E911 webpage of the Washington Military Department’s Emergency Management Division, available at: <https://mil.wa.gov/e911>. The population statistic is from the Washington Office of Financial Management, “State Population Steadily Increases, Tops 7.7 Million Residents in 2021” (6/30/21), available at: <https://ofm.wa.gov/about/news/2021/06/state-population-steadily-increases-tops-77-million-residents-2021>

1 seamlessly to connect every 911 caller almost instantly to the most appropriate
2 responding authority, on a 24/7, always-on basis.

3 In 2019 (the latest published data), over 5.3-million 911 calls were delivered
4 over the Washington E911 system, and 6.8-million 911 calls were delivered in
5 2018.¹¹ Those figures equate to some 14,500 and 18,600 calls per day on average,
6 respectively, indicating how important the system is to serve the public's welfare.

7
8 **Q. What state authority oversees the coordination of Washington's E911 system?**

9 A. The State Enhanced 911 Coordination Office ("SECO") within the Emergency
10 Management Division of the Washington Military Department ("WMD") is
11 Washington's state-level E911 authority.¹² SECO is responsible for the overall
12 coordination of the E911 system, and for the funding, planning, management, and
13 operations of certain service components. In this role, SECO works cooperatively
14 with numerous other regional and local public safety authorities that participate in
15 the system, including those operating the PSAPs. One of WMD's primary
16 responsibilities is to contract with a telecommunications company to provide the
17 statewide backbone network for the E911 system, known as an Emergency Services
18 Internet Protocol Network ("ESInet").

19

¹¹ Washington state reported 5,317,793 calls were delivered to primary PSAPs in the state during calendar year 2019. *See*, Webber, Exh. JDW-7 at 11. *See also*, Webber, Exh. JDW-8 at 3, 11 (showing 6,802,791 calls to primary PSAPs for 2018).

¹² *See*, RCW 38.52.005; RCW 38.52.010; RCW 38.52.030 ("(7) The director, through the state enhanced 911 coordinator, shall coordinate and facilitate implementation and operation of a statewide enhanced 911 emergency communications network."); RCW 38.52.520 (establishing the state enhanced 911 coordination office in the emergency management division).

1 **Q. What is an ESInet?**

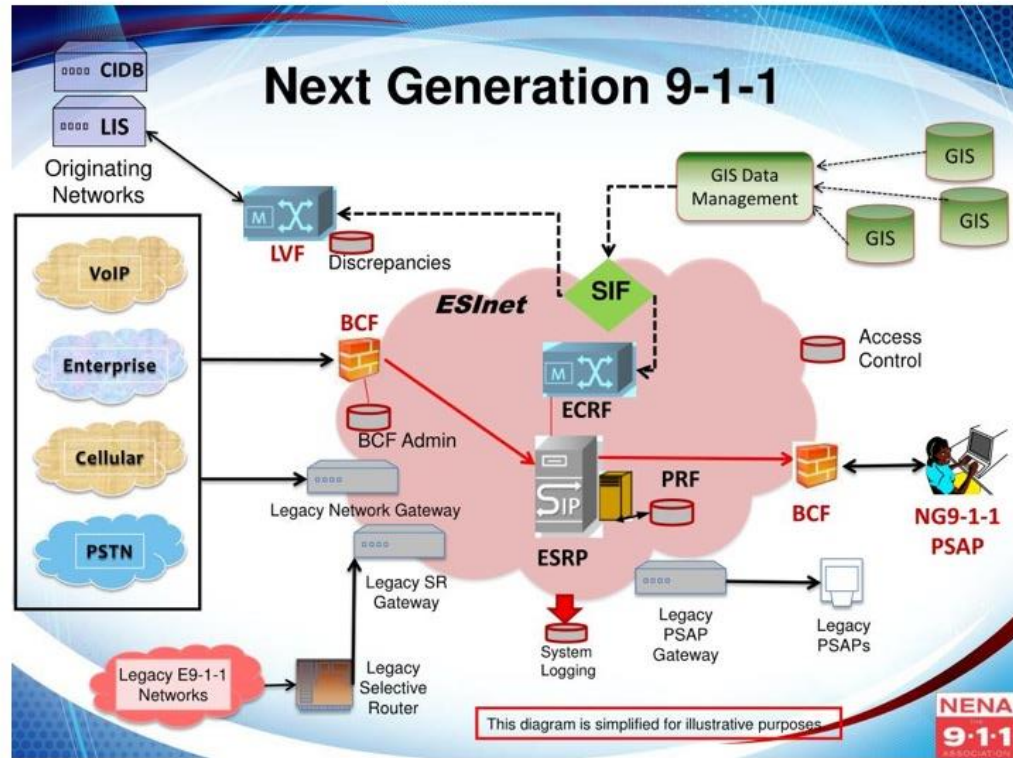
2 A. An ESInet is an Internet Protocol (“IP”)-based digital transport network used for
3 emergency services communications, i.e., 911 calls and associated data, that can be
4 shared by a state’s public safety agencies.¹³ It provides 911 call routing, transport,
5 interoperability, security, and related services. To do this, an ESInet connects
6 originating services providers (“OSPs”), including traditional local exchange carriers
7 (“LECs”), mobile wireless services providers, and CLECs, among others, to the
8 PSAPs. As the figure below suggests, having a modern ESInet is also an essential
9 prerequisite to providing advanced Next Generation 911 (“NG911”) capabilities,
10 e.g., the ability to receive 911 calls in the form of text messages and (in the future)
11 video calls in addition to voice telephony.¹⁴

12

¹³ Webber, Exh. JDW-9 at 2-4.

¹⁴ See, 47 C.F.R. § 942(e)(5) (defining “Next Generation 9-1-1 Services”).

Figure 1: Representative Next Generation 911 System¹⁵



2

3 **Q. How has the ESInet concept been implemented in Washington?**

4 A. In Washington, WMD contracted with CenturyLink to build and operate the state's
 5 first ESInet, ESInet I, in June 2009. Then, in June 2016, WMD contracted with
 6 TSYS to build, maintain, and operate a new ESInet, known as ESInet II, that would
 7 support NG911-compliant capabilities. CenturyLink and TSYS entered into a service
 8 agreement to undertake a phased transition of 911 operations from ESInet I to ESInet
 9 II, by the end of which TSYS would assume responsibility for the handling and
 10 processing all E911 calls in Washington state.¹⁶ WMD announced in August 2020

¹⁵ Webber, Exh. JDW-10 at 3.

¹⁶ See also, Exh. JDW-3C at 8-10.

1 that ESInet II was complete and beginning to provide NG911 services, including text
2 to E911.¹⁷

3

4 **Q. What was the status of the transition from ESInet I to ESInet II at the time of**
5 **the December 2018 outage?**

6 A. Simply put, at the time of the outage, the transition was not yet complete. The
7 transition status at the time of outage is described in detail in Staff's Investigation
8 Report, based upon the contracts executed by WMD, TSYS, and CenturyLink for
9 establishing and transitioning to ESInet II. The Report observes that:

10 During phase one, E911 service was provided in a segmented manner, where
11 the termination of E911 calls to PSAPs was split between PSAPs still
12 "connected" to CenturyLink's ESInet 1 and those PSAPs "connected" to
13 Comtech's ESInet 2. As the originating service provider, CenturyLink [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Furthermore, regardless of whether a PSAP was
18 receiving service from CenturyLink or Comtech, during phase one all
19 [REDACTED]
[REDACTED]¹⁸

21

22 **Q. Returning to the importance of the Washington E911 system for the safety and**
23 **protection of the state's citizens, can this be traced back to the original**
24 **Communications Act of 1934?**

25 A. Yes. The impetus for creating 911 capabilities can be traced all the way back to the
26 federal Communications Act of 1934, which among its purposes included that of

¹⁷ Webber, Exh. JDW-11.

¹⁸ Webber, Exh. JDW-3C at 8-10.

1 “promoting safety of life and property through the use of wire and radio
2 communications...”–which remains in full force today.¹⁹ While the concept of a
3 unified three-digit “911” dialing code to access emergency services dates back to the
4 late 1960s, it took decades for the service to expand across the U.S. and to evolve
5 into the integrated, flexible, and generally robust system the country enjoys today.²⁰
6

7 **Q. Have the capabilities of 911 systems increased as telecommunications
8 technology has improved over time?**

9 A. Yes, such capabilities have improved in several important respects over the past few
10 decades. One key development that greatly increased the effectiveness of 911
11 systems was the deployment of E911 capability, which automatically identified the
12 geographic location of the calling party and relayed that location to the PSAP in
13 order to expedite emergency responders’ ability to get to the site of the emergency.²¹
14 In 1991, the Washington Legislature passed House Bill 1938 (“HB 1938”). HB 1938
15 directed WMD to upgrade to an E911 capable system.²²

16 Further evolution of the E911 system, both in Washington and nationwide,
17 has included integrating wireless telephone service into the system (and solving the
18 caller location identification issues that mobile wireless service have presented),
19 expanding to encompass voice over internet protocol (“VoIP”) service, and most
20 recently, evolving towards the NG911 capabilities that I discussed above.

¹⁹ 47 U.S.C. § 151.

²⁰ Webber, Exh. JDW-12.

²¹ See, E911 webpage of the Washington Military Department’s Emergency Management Division at:
<https://mil.wa.gov/e911>

²² E.S.H.B. 1938, 52nd Leg., Reg. Sess. (Wa. 1991).

1 **Q. Have the Washington Legislature and the Commission recognized the**
2 **importance of the state’s E911 system to the safety and welfare of its residents?**

3 A. Yes. RCW 38.52.500 states that “[t]he legislature finds that a state-wide emergency
4 communications network of enhanced 911 telephone service, which allows an
5 immediate display of a caller’s identification and location, would serve to further the
6 safety, health, and welfare of the state's citizens, and would save lives.”²³ The
7 Commission subsequently established E911 requirements for all local exchange
8 telephone companies in the state, including obligations that LECs make E911 access
9 available to their customers and transmit callers’ emergency location identifier
10 number (“ELIN”) along with their call into the E911 system.²⁴

11 More recently, the Commission reaffirmed the critical nature of E911
12 services to the state’s residents in the context of an order addressing a CenturyLink
13 E911 system outage in 2014:

14 The outage on April 9-10, 2014, was a potentially life-threatening incident.
15 The citizens of this state reasonably rely on their ability to access emergency
16 services by dialing 911. Their inability to do so for even a brief period of
17 time poses a serious threat to public health, safety, and welfare, not just a
18 violation of statute and Commission rules.²⁵

19
20 **Q. As 911 systems have evolved and become more sophisticated over time, have**
21 **they also become more complex?**

²³ RCW 38.52.500.

²⁴ WAC 480-120-450. *See also, In re Amending, Adopting and Repealing Chapter 480-120 WAC Relating to Telephone Companies*, Docket UT-990146, Gen. Order R-507 (Dec. 16, 2002).

²⁵ *Wash. Utils. & Transp. Comm’n v. Qwest Corporation d/b/a CenturyLink QC*, Docket UT-140597, Order 03, at 4, ¶ 9 (Feb. 22, 2016).

1 A. Yes. As a result of the increased technological sophistication of E911 networks and
2 their expansion into additional communications modes beyond traditional wireline
3 voice telephone, combined with the general growth in competition in the industry,
4 today's 911 systems are significantly more complex, with a greater number of
5 service providers and other vendors involved, some with quite specialized roles.

6 The Commission recognized and described this complexity in comments it
7 filed with the FCC in March 2015 in response to that agency's proceedings
8 examining 911 Governance and Accountability.²⁶ The Commission's comments
9 observed that "technological and marketplace changes are altering the manner in
10 which some components of 911 service are handled, including increasing reliance on
11 network components and technology that are multi-state in nature."²⁷ The
12 Washington Commission went on to say:

13 As the [Federal Communications] Commission is aware, delivery of 911
14 services has evolved as niche entities have increasingly been engaged by
15 traditional 911 service providers to assume a variety of network and service
16 delivery functionalities. Although this evolution may well be appropriate to
17 streamline and achieve economies in the provision of such 911 service
18 delivery capabilities, this change also reflects a more diverse and complex
19 condition that warrants a greater level of oversight. Many of the emerging
20 911 specialized providers merely serve as contractors or sub-agents to other
21 traditional 911 service providers with overall contractual responsibility to
22 public safety entities and the UTC does not believe such 911 service
23 providers should escape scrutiny and responsible oversight given the
24 importance of safe and reliable 911 services.²⁸

²⁶ Webber, Exh. JDW-13.

²⁷ Webber, Exh. JDW-13 at 4.

²⁸ Webber, Exh. JDW-13 at 7.

1 As will become clear later in my testimony, the Commission’s observations in its
2 comments to the FCC remain very timely and relevant factors to consider when
3 evaluating the December 2018 outage.

4 **IV. THE CAUSE OF THE DECEMBER 27-29, 2018 OUTAGE**

5
6 **A. The primary and avoidable cause of the Washington E911 network**
7 **outage in December 2018 was CenturyLink’s failure to disable unused**
8 **communications paths, [REDACTED]**
9 **[REDACTED], between nodes on its [REDACTED]. Those**
10 **“unlocked” [REDACTED] were the primary reason that just four malformed**
11 **packets could escalate into a debilitating “packet storm” that crippled**
12 **the [REDACTED] across dozens of states for over two days, and led to**
13 **the outage experienced on Washington’s E911 system.**

14
15
16 **Q. Please describe the December 2018 outage that impacted Washington’s E911**
17 **communications system.**

18 **A.** In the early morning of December 27, 2018, Washington began undergoing a state-
19 wide outage of its E911 emergency services communications system that lasted more
20 than two days into December 29, 2018. Washington residents and businesses
21 attempting to make E911 calls during that time experienced fast busy signals or were
22 unable to connect.²⁹ Many thousands of calls failed to be completed to
23 Washington’s PSAPs, and other calls that were connected had impairments to the
24 delivery of callers’ location information from the E911 system’s Automatic Location
25 Information (ALI) databases.

26 At the time of the outage, CenturyLink had been the incumbent E911 service
27 provider in Washington for several years but was in the process of transferring that

²⁹ Webber, Exh. JDW-3C at 20-21.

1 role to a new provider, TSYs. The Washington E911 disruption was part of a much
2 wider outage occurring at that time on one of CenturyLink's fiber-based long-haul
3 transport networks, referred to as the [REDACTED]. The [REDACTED] outage
4 entirely disrupted or impaired many CenturyLink services in multiple states and had
5 rippling effects on other service providers relying upon that network, including 911
6 service providers in several states in addition to Washington.³⁰ CenturyLink
7 estimated that its [REDACTED] outage caused over 12 million calls across the
8 country to be blocked or degraded.³¹

9
10 **Q. Have you investigated the causes of the CenturyLink [REDACTED] outage and**
11 **its relationship to the failures in the Washington E911 system during December**
12 **27-29, 2018?**

13 A. Yes. I reviewed all of the information pertaining to that network outage that Staff
14 obtained and shared with QSI, including relevant discovery responses, the August
15 2019 Report of the FCC's Public Safety and Homeland Security Bureau, Staff's
16 December 2020 Investigation Report, CenturyLink's February 2019 Root Cause
17 Analysis filed in Docket UT-170042, and post-outage reports and other
18 documentation from CenturyLink's network equipment vendor Infinera Intelligent
19 Transport Networks ("Infinera").

³⁰ Webber, Exh. JDW-4 at 8-9. *See also*, Webber, Exh. JDW-14C at 4 (stating that the outage [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]).

³¹ Webber, Exh. JDW-4 at 8-9.

1 After learning that CenturyLink experienced a [REDACTED]
2 [REDACTED]—QSI also
3 gathered and reviewed information concerning that network outage, which further
4 informed my analysis and conclusions concerning the December 2018 outage.
5

6 **Q. What is your understanding of the events that led to the December 2018 outage**
7 **on CenturyLink’s [REDACTED]?**

8 A. Most of the circumstances and key facts concerning that outage are reasonably well
9 described in the documents referenced above. In particular, the FCC report provides
10 a good in-depth description of the relevant aspects of the architecture of the [REDACTED]
11 [REDACTED] and how the “packet storm” that drove the outage began and spread
12 throughout that network with paralyzing effects.³² Rather than recapitulate all of
13 those facts here, I will focus on what I consider to be the key factors that led to the
14 [REDACTED] failure during that period.

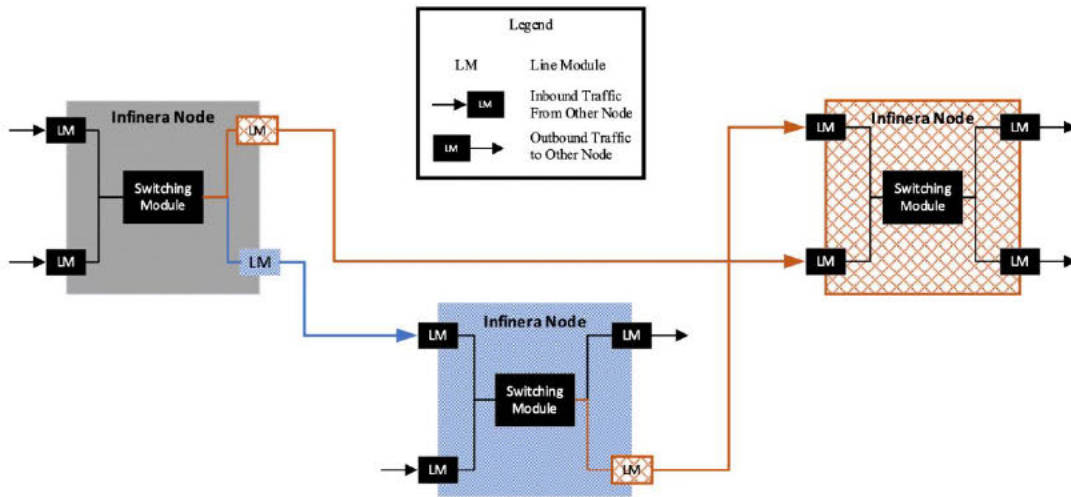
15 The main elements of CenturyLink’s [REDACTED] are nodes supplied by
16 Infinera that provided optical switching between line modules.³³ The following
17 simplified diagram from the FCC’s Report shows three Infinera nodes and illustrates
18 how their switching modules can direct traffic from one node to another by choosing
19 paths between different line modules.
20

³² Webber, Exh. JDW-4 at 6-10. Staff’s Investigation Report draws upon the FCC report to provide a briefer summary of those aspects of the December 2018 event. *See*, Webber, Exh. JDW-3C at 16-17.

³³ To be clear, my focus here is on describing how the [REDACTED] and Infinera equipment functioned at the time of the outage, although my understanding is that it generally functions the same way presently as well.

1

Figure 2: Infinera Switching Nodes and Line Modules³⁴



2

3 But in addition to the connections between line modules that carry customer traffic,

4 Infinera line modules are also connected by communications paths [REDACTED]

5 [REDACTED].³⁵ [REDACTED] are not intended to carry

6 customer traffic, but instead are separate channels intended to be used to transmit

7 control plane communications for traffic management purposes, e.g., to

8 automatically reroute traffic quickly in the event of a node failure.³⁶ The following

9 diagram from Infinera illustrates how [REDACTED]s linked together line modules from

10 different switching nodes and allowed them to send packets directly from one line

11 module to another.

12

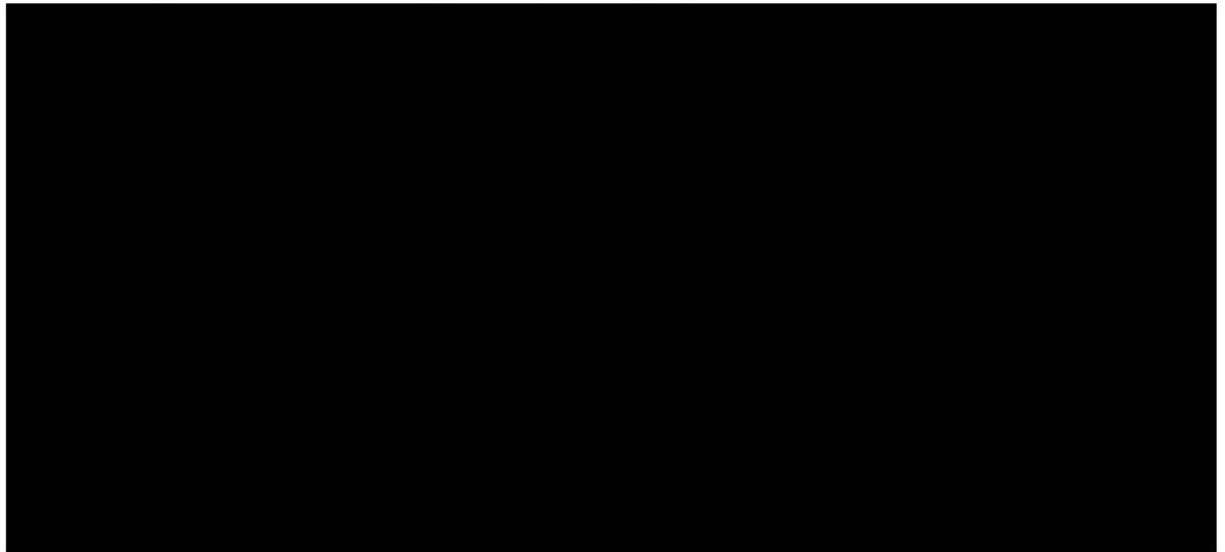
³⁴ Webber, Exh. JDW-4 at 6.

³⁵ The FCC Report refers to them as “proprietary internode management channels.” See, Webber, Exh. JDW-4 at 6. Staff’s Investigation Report follows that terminology. See, Webber, Exh. JDW-3C at 16-18.

³⁶ Webber, Exh. JDW-4 at 6.

1

Figure 3: Illustration of [REDACTED] Linking Infinera Line Modules³⁷



2

3 Infinera's [REDACTED] have two basic settings: enabled/disabled and configured/not
4 configured.³⁸ The FCC's report revealed two critical facts about the [REDACTED]:

5 As the supplier of these nodes, Infinera provides its customers – including
6 CenturyLink in this case – with the proprietary management channel [REDACTED]
7 enabled by default. CenturyLink was aware of the channel but neither
8 configured nor used it.³⁹

9 The fact that the [REDACTED] [REDACTED] were enabled and thus able to send traffic
10 between line modules, even though CenturyLink was not using them, was a key
11 driver of the outage.

12

³⁷ Webber, Exh. JDW-5C at 6.

³⁸ Webber, Exh. JDW-6C at 1-2 (“With regard to Infinera equipment installed on the networks of [CenturyLink] and its affiliates, Infinera designed its network switching equipment in a manner which enabled the management channel on each line card as a default setting. The only possible settings for the management channel are enabled or disabled, and configured or not configured.”). CenturyLink is using the term “management channel” to refer to the [REDACTED].

³⁹ Webber, Exh. JDW-4 at 6.

1 Q. Did the [REDACTED] outage originate from the [REDACTED] themselves?

2 A. No, not directly. The [REDACTED] outage began from a small number of
3 “spontaneously generated” malformed packets (literally, four of them)⁴⁰ that, among
4 other attributes, were: (a) designated to be broadcasted to all connected nodes, rather
5 than destined for a particular node; (b) were larger than 64 bytes in size; and (c) had
6 no expiration date. Because of these unusual characteristics, these packets were able
7 to “escape” through the unused, but enabled, [REDACTED] and thus get communicated to
8 other connected line modules.⁴¹ This circumstance quickly led to a crippling “packet
9 storm,” as the condition is known in the industry.

10

11 Q. Can you describe the packet storm as it occurred on the [REDACTED]?

12 A. Yes. Because the [REDACTED] has many line modules interconnected through
13 [REDACTED], the malformed broadcast packets easily propagated through those channels
14 and replicated when they arrived at another node. This situation created a positive
15 feedback loop that quickly grew into the exponential cascade of packets that
16 constitutes a “packet storm.”⁴² Infinera characterized the problem this way in an
17 advisory it circulated days after the event:

18

[REDACTED]

19

[REDACTED]

20

[REDACTED]

21

[REDACTED]

⁴⁰ Webber, Exh. JDW-4 at 6.

⁴¹ See, Webber, Exh. JDW-4 at 7 (providing details of the packet size filter and other condition checks that the malformed packets managed to evade due to their combination of attributes I have described above).

⁴² Webber, Exh. JDW-4 at 7. I note that the FCC report never used the term “packet storm” even though both CenturyLink and Infinera have characterized the outage as caused by a packet storm.

2 [REDACTED]⁴³

3 This packet storm quickly consumed and exhausted the processing capacity of
4 multiple nodes, disrupting the [REDACTED] routing management and traffic
5 flows. The nodes became unable to maintain their internal synchronization, and
6 consequently lost their ability to route and transmit traffic.⁴⁴ And because the packet
7 storm also prevented CenturyLink’s network administrators from gaining access to
8 those overloaded nodes remotely to diagnose and take steps to rectify the problem,
9 the outages were prolonged considerably.⁴⁵

10

11 **Q. How did CenturyLink regain control over the [REDACTED] and eliminate the**
12 **packet storm?**

13 A. The FCC Report recounts several actions that CenturyLink took to restore the [REDACTED]
14 [REDACTED], but the most essential step was that CenturyLink progressively disabled
15 more and more of the [REDACTED] over time, thereby preventing them from allowing any
16 more malformed packets to be transmitted across nodes.⁴⁶ CenturyLink described the
17 process in these terms in its February 2019 Root Cause Analysis:

18 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

⁴³ Webber, Exh. JDW-5C at 14.
⁴⁴ Webber, Exh. JDW-4 at 7-8.
⁴⁵ Webber, Exh. JDW-4 at 8.
⁴⁶ Webber, Exh. JDW-4 at 8.
⁴⁷ Webber, Exh. JDW-14C at 2.

1 That Analysis went on to state:

2 [REDACTED]
3 [REDACTED]
4 [REDACTED]

5

6 **Q. Based upon the analysis you just supplied, what is your opinion concerning the**
7 **cause of the December 2018 outage on CenturyLink's [REDACTED]**

8 A. The outage on the [REDACTED] was a complex event with multiple contributing
9 factors. In my view, however, the primary and avoidable cause of the outage was the
10 fact that CenturyLink had been operating the network with the [REDACTED]
11 [REDACTED] enabled and “unlocked,” despite not using them—thereby leaving the
12 network vulnerable to a packet storm. While the creation of malformed packets was
13 a necessary factor as well, the difference is that their creation was not well
14 understood and easily avoidable by Infinera and CenturyLink. In contrast, disabling
15 the [REDACTED] was entirely within CenturyLink’s control, and in fact, CenturyLink did
16 exactly that immediately after the crippling outage occurred.

17 As I describe next, CenturyLink had a stark warning of its exposure to that
18 vulnerability, when its parallel [REDACTED]
19 [REDACTED] before the outage at issue here.

20

21 **Q. Earlier in your testimony, you mentioned that CenturyLink’s [REDACTED] had**
22 **experienced an outage in [REDACTED]. Can you summarize what happened to**
23 **the [REDACTED] at that time?**

⁴⁸ Webber, Exh. JDW-14C at 2.

1 A. Yes. The [REDACTED] is another one of CenturyLink's six national transport
2 networks, originally owned and operated by Level 3 prior to CenturyLink's
3 acquisition of Level 3. [REDACTED]

4 [REDACTED]
5 [REDACTED].⁴⁹ As with the [REDACTED], the default setting
6 for Infinera's line cards was to have the [REDACTED] enabled.⁵⁰

7 As described in Infinera's subsequent investigation report concerning this
8 other network incident, [REDACTED]

9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED].⁵¹

18
19 **Q. Based on your review of the events you just described, what was the cause of**
20 **the [REDACTED] outage?**

⁴⁹ Webber, Exh. JDW-6C at 18-19.

⁵⁰ Webber, Exh. JDW-6C at 1.

⁵¹ Webber, Exh. JDW-5C at 3-5. [REDACTED]

[REDACTED]
[REDACTED] See, Webber, Exh. JDW-14C at 2.

1 A. As in the case of the [REDACTED] a number of factors contributed to this outage.

2 Once again, however, it is clear to me that [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED] And just as was the case for the [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]:

9 [REDACTED]

■ [REDACTED]

■ [REDACTED].⁵²

12 And as I discuss later in my testimony, immediately after [REDACTED]

■ [REDACTED]

■ [REDACTED]

15

16 **Q. In response to Staff's discovery concerning the operational similarities and**

17 **differences between the [REDACTED], CenturyLink has claimed**

18 **that [REDACTED]**

■ [REDACTED]

■ [REDACTED]

⁵² Webber, Exh. JDW-5C at 3.

⁵³ Webber, Exh. JDW-5C at 9.

1 [REDACTED] Is that an accurate
2 characterization of [REDACTED]?

3 A. No, not at all. I do not find that statement to be accurate, nor do I find CenturyLink's
4 similar assertions in response to other Staff discovery to be accurate.⁵⁵ Although the
5 FCC Report did not refer to the [REDACTED] outage, when we
6 observed that it was noted in [REDACTED]
7 [REDACTED],⁵⁶ Staff propounded follow-up discovery, including a request
8 that CenturyLink provide all documents, emails, and other communications
9 generated in the course of the investigations done to determine whether there was a
10 related, underlying fault in the two outages. CenturyLink responded that it had no
11 such documents, other than what it had already produced, and that "[i]t is
12 [CenturyLink]'s recollection (acknowledging, of course, that three years have
13 passed) that much of the discussion between Infinera and [CenturyLink] was verbal
14 and not in writing."⁵⁷

15 Consequently, the only written documents from Infinera that CenturyLink
16 produced addressing the causes of the [REDACTED] outage [REDACTED]

⁵⁴ Webber, Exh. JDW-6C at 18. I note also that immediately following the quoted statement, the response continues [REDACTED]

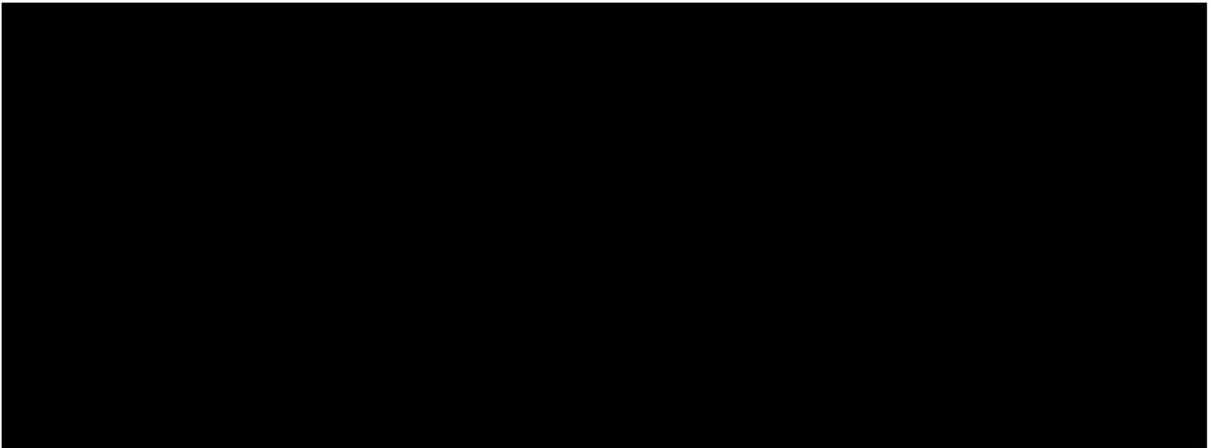
⁵⁵ Webber, Exh. JDW-6C at 16 (stating in part that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]); Webber, Exh. JDW-6C at 2 (stating in part that "While the software upgrade, not enablement of the management channel of the line card, created the issue, the management channel permitted the keepalive packets to propagate." and "After the Level 3 network event, Infinera determined that its software upgrade (version 16.2) had created the problem.").

⁵⁶ See, Webber, Exh. JDW-14C at 2 [REDACTED]
[REDACTED].

⁵⁷ Webber, Exh. JDW-6C at 14.

1 [REDACTED] (cited above) and Infinera’s incident report immediately following the
2 [REDACTED] outage.⁵⁸ Contrary to CenturyLink’s sweeping statement regarding
3 Infinera’s guidance quoted above, neither document states that [REDACTED]
4 [REDACTED]
5 [REDACTED]. Rather, [REDACTED]
6 [REDACTED] and further
7 elaborates on this in the subsequent section describing [REDACTED]

8 *Figure 4:* [REDACTED] [REDACTED]



9
10 Accordingly, [REDACTED]
11 [REDACTED]
12 [REDACTED] did not “cause” them: instead, as explained above,
13 [REDACTED]
14 [REDACTED]
15 [REDACTED].⁶¹ Similarly, [REDACTED]

⁵⁸ Webber, Exh. JDW-5C at 1-12; 16-41.
⁵⁹ Webber, Exh. JDW-5C at 3.
⁶⁰ Webber, Exh. JDW-5C at 5.
⁶¹ Webber, Exh. JDW-5C at 5.

█ [REDACTED]
█ [REDACTED]
█ [REDACTED].⁶²

4

5 **Q. Mr. Webber, earlier in your testimony you mentioned that immediately after**
6 **the [REDACTED] packet storm, Infinera [REDACTED]**

█ [REDACTED] **Have you been**
8 **able to confirm that this action was carried out?**

9 A. No. When we asked CenturyLink whether this action was performed on its [REDACTED]
10 [REDACTED], it responded that “[CenturyLink] is not in a position to represent all steps
11 taken by Infinera to [REDACTED]

12 [REDACTED] I find this response to be evasive and
13 incomplete given that the first subpart of Staff Data Request No. 24(a) simply asked

14 [REDACTED] As the owner and manager of the network,
15 CenturyLink surely should know the answer to this question.⁶⁴ CenturyLink further
16 responded that [REDACTED]

█ [REDACTED] but did not
18 provide any document, email, or other written communication between CenturyLink
19 and Infinera between the time of the two 2018 outages to substantiate that claim,
20 despite promising that it would supplement its prior response to Staff’s data request.

⁶² Webber, Exh. JDW-5C at 23.

⁶³ Webber, Exh. JDW-6C at 16.

⁶⁴ Webber, Exh. JDW-6C at 15.

⁶⁵ Webber, Exh. JDW-6C at 16.

1 I also find it questionable that, in response to Staff Data Request No. 3,
2 CenturyLink simultaneously claims that: (1) “Infinera advised [CenturyLink] that it
3 need not close the management channel...”; and (2) “Infinera likewise advised
4 [CenturyLink] to keep the management channel enabled because the Infinera
5 network switching equipment in [CenturyLink]’s network was operating using
6 software version 15.3.3.”⁶⁶ Those purported recommendations are not equivalent,
7 and neither I nor the Commission can confirm which, if either, of these
8 recommendations Infinera actually made without further evidence from
9 CenturyLink.

10
11 **Q. After the [REDACTED] packet storm occurred on CenturyLink’s [REDACTED]
12 [REDACTED], and was stopped by locking down its [REDACTED],
13 was it prudent for CenturyLink to continue to leave its [REDACTED] on the [REDACTED]
14 [REDACTED] unlocked (enabled) and capable of unleashing a packet storm, when it
15 was not using those channels and there was no downside to disabling them?**

16 **A. No. CenturyLink, rather than its vendors, is ultimately responsible for managing its
17 networks in a prudent manner.⁶⁷ Given that [REDACTED]**

18 [REDACTED]
19 [REDACTED], I see no reason why CenturyLink chose to keep the [REDACTED] on its

⁶⁶ Webber, Exh. JDW-6C at 2.

⁶⁷ See, *Wash. Utils. & Transp. Comm’n v. Qwest Corporation d/b/a CenturyLink QC*, Docket UT-140597, Order 03, at 9, ¶ 25 (Feb. 22, 2016) (“What is important for our review is to ensure that CenturyLink has adequate management and oversight systems in place to both reduce the risks of such errors occurring and also to have systems in place to provide awareness of outages and to restore 911 service as rapidly as possible. This applies to both the Company itself and to any contractor or vendor such as Intrado. In other words, we require regulated companies to implement measures that are reasonable under the circumstances to minimize service disruptions and other violations of Commission requirements.”).

1 [REDACTED] unlocked and therefore exposed to that same grave and consequential
2 vulnerability.

3
4 **Q. Does the FCC work cooperatively with the telecommunications industry to**
5 **develop and disseminate best practices concerning network reliability and**
6 **security issues?**

7 A. Yes, it does. In January 1992, the FCC organized the Network Reliability Council
8 (“NRC”) “following a series of major service outages in various local exchange and
9 interexchange wireline telephone networks. The Commission established the Council
10 to study the causes of service outages and to develop recommendations to reduce
11 their number and their effects on consumers.”⁶⁸ After nearly fifteen years of service,
12 the NRC was superseded by the Communications Security, Reliability, and
13 Interoperability Council (“CSRIC”), which continues that work but with a wider
14 scope. CSRIC describes its mission as “to make recommendations to the
15 Commission to promote the security, reliability, and resiliency of the Nation’s
16 communications systems.”⁶⁹ CSRIC regularly issues reports with recommendations
17 based upon best practices seen in the industry. CenturyLink itself participated in the
18 membership of several CSRIC councils (e.g., CSRIC Councils III and V).⁷⁰

19

⁶⁸ FCC’s webpage on the NRIC, available at: <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-9>

⁶⁹ FCC’s CSRIC webpage, available at: <https://www.fcc.gov/CSRICReports>

⁷⁰ *Id.*

1 **Q. Did the FCC’s Public Safety and Homeland Security Bureau Report concerning**
2 **the CenturyLink December 2018 outage find that the Company failed to follow**
3 **CSRIC recommended best practices that could have prevented or mitigated**
4 **that outage?**

5 A. Yes. The Report found that “There are several best practices that could have
6 prevented the outage, or at least mitigated its effects.”⁷¹ The first recommendation it
7 makes is that “System features that are not in use should be turned off or disabled,”
8 citing to two specific CSRIC best practices.⁷² It goes on to explain:

9 In this case, the proprietary management channel [REDACTED] was enabled by
10 default so that it could be used if needed. While CenturyLink did not intend
11 to use the feature, it left it unconfigured and enabled. Leaving the channel
12 enabled created a vulnerability in the network that, in this case, contributed to
13 the outage by allowing malformed packets to be continually rebroadcast
14 across the network.⁷³

15 After the outage and publication of its Report, the PSHSB issued a Public Notice
16 reiterating to all network operators and service providers the importance of this best
17 practice and others bearing on that outage as steps that “could prevent or mitigate
18 similar outages in the future.”⁷⁴

19
20 **Q. Are there additional reasons not to keep an unused network function enabled?**

⁷¹ Webber, Exh. JDW-4 at 15.
⁷² Webber, Exh. JDW-4 at 15 n. 40 (citing CSRIC Best Practices 11-6-5170 and 11-8-8000). *See also*, Webber, Exh. JDW-15 at 9-6-5170 and 9-8-8000.
⁷³ Webber, Exh. JDW-4 at 15.
⁷⁴ Webber, Exh. JDW-16 at 2,

1 A. Yes. Separately from the PSHSB action, the U.S. National Security Agency (“NSA”)
2 has issued an advisory in August 2020 for Hardening Network Devices on networks.

3 That advisory states that:

4 Hardening network devices reduces the risk of unauthorized access into a
5 network’s infrastructure. Vulnerabilities in device management and
6 configurations present weaknesses for a malicious cyber actor to exploit in
7 order to gain presence and maintain persistence within a network.
8 Adversaries have shifted their focus from exclusively exploiting traditional
9 endpoints to increasingly exploiting specialized and embedded devices,
10 including routers and switches. They do this through manipulating
11 weaknesses in configurations, controlling routing protocols, and implanting
12 malware in the operating systems.⁷⁵

13 In its Service Security section, the advisory states:

14 All networking devices, including routers and switches, come equipped with
15 services turned on when they are received from the manufacturer. Disabled
16 services cannot be exploited by an adversary. Therefore, all unnecessary
17 services should be disabled.⁷⁶

18 By failing to secure its [REDACTED] in this fashion—even after witnessing its [REDACTED]
[REDACTED] just ten months
20 earlier—CenturyLink perpetuated a known vulnerability to a massive packet storm
21 that ultimately led to the [REDACTED] serious and prolonged outage throughout
22 December 27-29, 2018, and its consequent debilitating impacts on the Washington’s
23 E911 system and the public it serves.

⁷⁵ Webber, Exh. JDW-17 at 1.

⁷⁶ Webber, Exh. JDW-17 at 1 (emphasis added).

1
2
3
4
5
6
7
8
9

V. IDENTIFICATION OF CIRCUITS IMPACTED BY THE CENTURYLINK OUTAGE

A. Four SS7 circuits provided by CenturyLink riding on its [REDACTED] [REDACTED] failed due to the packet storm and prevented TSYS and the PSAPs it served from completing E911 calls and obtaining callers' address information for several extended periods of time during that two-day December 2018 outage period.

10 Q. Can you explain the difference between the voice paths and the Signaling
11 System 7 ("SS7") circuits that comprise the TSYS ESInet II system?

12 A. Yes. Since its widespread adoption in the 1970s, telephony networks have used a
13 signaling technology called SS7 to route voice calls.⁷⁷ SS7 is called an "out-of-band"
14 signaling system that relies on communications over separate paths from those of the
15 calls that it is guiding to their destinations. CenturyLink and TSYS relied on SS7 to
16 route the E911 calls traversing their ESInets during the outage period. In contrast to
17 the older method of "in-band" signaling, in which the originating caller's switch
18 begins the process of routing a call through the telephone network as soon as the
19 digits to reach the called party are dialed, under SS7 the full call route is set up, via
20 an exchange of well-defined messages over those separate SS7 links to the final
21 switch which will terminate the call, before the call is sent anywhere. Once that
22 terminating switch accepts the proposed call and its acceptance reaches the
23 originating switch, the call path is established, connecting the two parties. When one

⁷⁷ There are now more advanced signaling protocols based upon IP technology, such as SigTran, that are superseding SS7, but they are not used to support calls to the PSAPs on ESInet II. *See*, Webber, Exh. JDW-18C at 8 ("No, [CenturyLink] did not use SIGTRAN for any SS7 connections."). My understanding is that CenturyLink denied TSYS' request to use IP-based signaling to support the calls terminating to PSAPs on the ESInet II during the transition. *See, e.g.*, Webber, Exh. JDW-19C at 3; Webber, Exh. JDW-20C at 2-4.

1 of the parties hangs up, a similar exchange of messages occurs over the SS7 links to
2 tear down that voice path, leaving those facilities idle until needed for another call.
3 And as I discuss later in my testimony, SS7 is a very flexible technology that can
4 perform many other functions, including transmitting the geographic address of a
5 person dialing 911 to the PSAP receiving an emergency call, in order to speed the
6 response time of the appropriate public safety agency.

7
8 **Q. Are SS7 systems typically designed to serve a single state, with all of the**
9 **associated signaling, switching, transmission and other supporting facilities**
10 **confined to a state's borders?**

11 A. No. To the contrary, SS7 systems instead tend to be multi-state in nature, both in
12 terms of the geographic areas they serve and the extent and scope of their facilities.
13 For example, Transaction Network Services Inc. ("TNS"), which is the provider of
14 SS7 services used by both CenturyLink and TSYs for their ESInets (as I discuss
15 further below), operates a multi-state network.

16
17 **Q. Does the fact that the signaling information conveyed by a multi-state SS7**
18 **system may cross state lines mean that the jurisdiction of all calls routed by**
19 **means of that system will necessarily be interstate, rather than intrastate?**

20 A. No. The FCC has a well-settled policy referred to as its "end-to-end analysis," by
21 which the jurisdiction of a call generally is determined by the location of its end
22 points, not by the particular geographic route that the call may traverse (setting aside

1 the signaling information exchanged in order to determine any particular call path).

2 As the FCC explained in its *Vonage* order:

3 Using an end-to-end approach, when the end points of a carrier’s service are
4 within the boundaries of a single state the service is deemed a purely
5 intrastate service, subject to state jurisdiction for determining appropriate
6 regulations to govern such service. When a service’s end points are in
7 different states or between a state and a point outside the United States, the
8 service is deemed a purely interstate service subject to the Commission’s
9 exclusive jurisdiction. Services that are capable of communications both
10 between intrastate end points and between interstate end points are deemed to
11 be “mixed-use” or “jurisdictionally mixed” services. Mixed-use services are
12 generally subject to dual federal/state jurisdiction, except where it is
13 impossible or impractical to separate the service’s intrastate from interstate
14 components and the state regulation of the intrastate component interferes
15 with valid federal rules or policies. In such circumstances, the Commission
16 may exercise its authority to preempt inconsistent state regulations that
17 thwart federal objectives, treating jurisdictionally mixed services as interstate
18 with respect to the preempted regulations.⁷⁸

19

20 **Q. If the SS7 component of an ESInet is disrupted by an outage, can voice calls still**
21 **be completed?**

22 A. No. Without a successful call setup, which the SS7 component must undertake, the
23 originating voice calls cannot be routed anywhere and will fail to connect. The
24 situation is roughly analogous to what can happen on a railroad when the system that
25 notifies train engineers that the rails ahead are free for their use: when that system
26 goes down, the trains cannot move anywhere (or else risk collisions), even though
27 the tracks and the trains themselves may be in perfect working order.⁷⁹

⁷⁸ See, e.g., *In re Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission*, WC Docket No. 03-211, Memorandum Opinion and Order, 19 FCC Rcd 22404, 22413, ¶ 17 (2004) (internal footnotes omitted).

⁷⁹ My point here is to emphasize the dependency of the underlying entity needing to be transported (calls, trains) on their routing information, not to dwell on possible differences in their signaling methods which might exist.

1 **Q. Are the SS7 links in an ESInet used for any other purpose than call routing?**

2 A. Yes. As a vital part of their E911 capabilities, an ESInet ensures that the trained call
3 recipient at a PSAP automatically receives the geographic location of the E911
4 caller. The PSAP obtains this information via a database query, or “dip”
5 (specifically, an 04-001 query) on the E911 system’s database containing Automatic
6 Location Identification (“ALI”) data for all telephony customers within the system’s
7 coverage area. [REDACTED]

■ [REDACTED]

■ [REDACTED]

10

11 **Q. Were the SS7 links used by either ESInet I or ESInet II disrupted by the**
12 **December 2018 network event?**

13 A. Yes. At a minimum, CenturyLink’s [REDACTED] failure clearly disrupted the SS7
14 links on which TSYS’ ESInet II relied, and that those disruptions were the primary
15 cause of the failed E911 calls throughout Washington. CenturyLink has repeatedly
16 denied that the SS7 links used by its ESInet I experienced any disruptions during the
17 December 2018 events.⁸¹ However, it is unclear at this point whether CenturyLink’s
18 claims are accurate. As explained in the next section of my testimony, it appears that
19 there *were* in fact E911 calls traversing ESInet I and destined for PSAPs still served
20 by CenturyLink that were impacted concurrent with the outages on ESInet II.

21

⁸⁰ Webber, Exh. JDW-3C at 9; Webber, Exh. JDW-19C at 5; and Webber, Exh. JDW-21C.

⁸¹ See, e.g., Webber, Exh. JDW-18C at 5-7.

1 **Q. Did you determine that there were separate disruptions during the December**
2 **2018 outage to the physical facilities that constituted the voice paths in the**
3 **ESInet I and ESInet II networks, as distinguished from their SS7 links?**

4 A. No. In response to discovery, both CenturyLink⁸² and TSYS have asserted that the
5 portions of their ESInets that actually transport and deliver E911 calls (as opposed to
6 their SS7 systems) remained functioning and able to complete calls during the entire
7 outage period. TSYS, for example, stated:

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]⁸³

12 **Q. Within the TSYS ESInet II system SS7 links, which specific circuits were**
13 **impacted by the December 2018 outage?**

14 A. The SS7 portion of TSYS' ESInet II system relied upon four circuits obtained from
15 CenturyLink to connect its E911 gateways serving Washington to the signaling
16 network for CenturyLink's ESInet I. All four of these circuits rode on CenturyLink's
17 [REDACTED] and failed as a result of the December packet-storm. The
18 failure of those four circuits disrupted TSYS' ability to route E911 calls handed-off
19 from CenturyLink, and impaired the PSAPs' ability to obtain location information
20 for those callers from the ALI databases. TSYS and CenturyLink's discovery
21 responses indicate the following details regarding these four circuits:
22
23

⁸² Webber, Exh. JDW-18C at 5-7.
⁸³ Webber, Exh. JDW-19C at 4.

1 • The four circuits established redundant connections between two TSYS gateways
2 for ESInet II, located in [REDACTED]

■ [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]⁸⁴ Those [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]⁸⁵

8 • According to TSYS, [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]⁸⁶ TSYS states that it ordered and provisioned [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]⁸⁷

13 TSYS provided a confidential diagram that [REDACTED]
■ [REDACTED]
■ [REDACTED]
■ [REDACTED]⁸⁸ See Figure 5
16 below for that diagram.

17
18

⁸⁴ Webber, JDW-22C at 4. *See also*, Webber, Exh. JDW-18C at 1-4.

⁸⁵ Webber, Exh. JDW-18C at 1-3. [REDACTED]
[REDACTED]

⁸⁶ Webber, Exh. JDW-22C at 1.

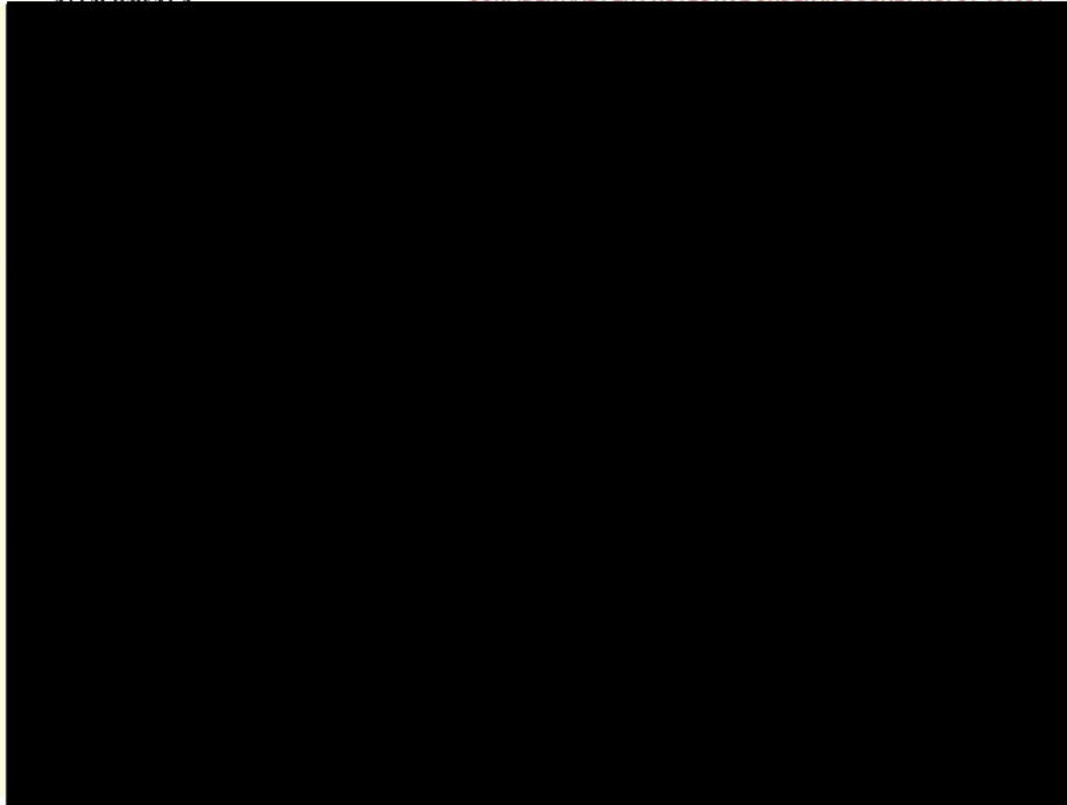
⁸⁷ *See*, Webber, Exh. JDW-22C at 1 (stating that “the capacity of each [REDACTED]”); Webber, Exh. JDW-22C at 4; and Webber, Exh. JDW-19C at 1 (stating that “[REDACTED]”).

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]⁸⁸ Webber, JDW-22C at 4.

1 *Figure 5: The Four CenturyLink Circuits Relied Upon by TSYS for SS7*
2 *Connectivity*
3

ATTACHMENT A

CONFIDENTIAL PER PROTECTIVE ORDER IN DOCKET NO. UT-181051



4

5

6

• TSYS further explained that its “intended redundancy was to have [REDACTED] [REDACTED], which is most certain using a single vendor since different vendors will not share information with one another about the physical paths they use.”⁸⁹

7

8

9

10

• CenturyLink admitted that all four of these circuits were provisioned on its [REDACTED] [REDACTED] which suffered the packet storm-driven major outage in December 2018.⁹⁰ CenturyLink also provided a diagram that [REDACTED]

11

12

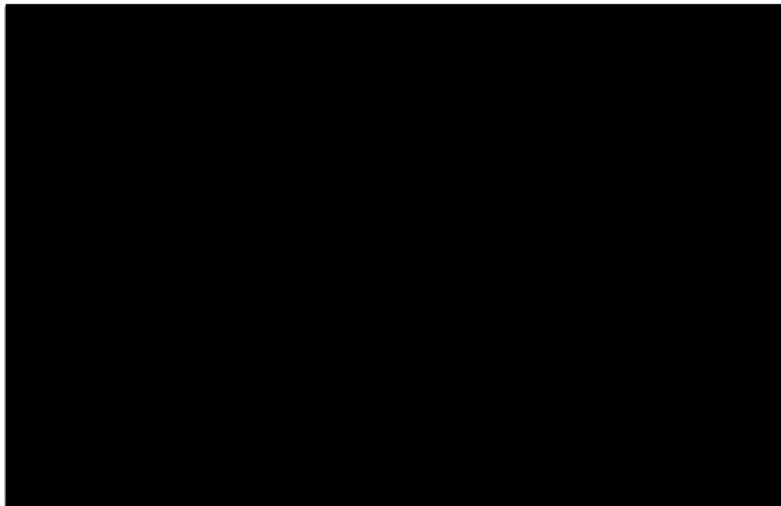
[REDACTED]

⁸⁹ Webber, Exh. JDW-19C at 2.

⁹⁰ Webber, Exh. JDW-6C at 7 (stating “The entire [CenturyLink] affiliated Infinera network was affected by the packet storm incident, and thus each of the TNS circuits was compromised.”); Webber, Exh. JDW-18C at 2 (stating, “It appears Comtech (and its contractor TNS) chose to utilize four separate circuits sitting on the same Infinera network....”).

1 [REDACTED] [REDACTED].⁹¹ Conceptually, because the outage on the [REDACTED]
2 disrupted the signaling network, the two systems could not “talk” to one another
3 through the SS7 network; and because of that lack of communication, voice calls (in
4 this case, E911 calls) could not connect to the relevant PSAPs as shown in the high-
5 level diagram below.

6 *Figure 6: The [REDACTED] Failure Disrupted TSYS’ Signaling and Call*
7 *Processing to PSAPs*



8
9 To summarize, because the CenturyLink [REDACTED] failed due to CenturyLink’s
10 inaction, TSYS’ SS7 network also failed, rendering ESInet II unable to set up,
11 connect, and complete E911 calls destined to PSAPs served by TSYS.⁹²

12
13 **Q. Did CenturyLink participate in the testing of these four circuits prior to their**
14 **acceptance by TSYS?**

15 **A. Yes. TSYS stated the following concerning the testing of those four circuits:**

16 [REDACTED]
[REDACTED]
[REDACTED]

⁹¹ Webber, Exh. JDW-18C at 4.

⁹² In addition, the impairment to the ESInet II signaling network adversely impacted the ability of PSAP dispatchers to obtain location information for E911 callers from the ALI database system.

1

[REDACTED]

4

On May 1, 2018, the first PSAPs in Washington cut over to TSYS, which is when the D-link circuits were effectively “turned on” to pass traffic between ESInet 1 to ESInet 2.⁹³

7

8

Q. Did CenturyLink know prior to the December 2018 outage that those four circuits were being used to provide SS7 links for an E911 system?

9

10

A. CenturyLink denies that it had that knowledge. In response to Staff discovery, CenturyLink replied:

11

12

During the December 2018 event, 911 calls to the CenturyLink PSAPs completed, but some calls to the Comtech PSAPs did not. Comtech utilized Transaction Network Systems (“TNS”) to provide Comtech SS7 services in support of Comtech’s 911 services in Washington. TNS submitted orders to CLC for dedicated facilities to use as SS7 links, but did not inform CenturyLink that these circuits would be used to provide SS7 service and/or to support 911 services. Prior to the outage, CLC was unaware that TNS was using circuits on CLC’s national transport network to provide SS7 functionality at all, let alone in support of Comtech’s 911 services in Washington.⁹⁴

13

14

15

16

17

18

19

20

21

22

23

However, TSYS asserted that communication between TSYS and CenturyLink a few months before the December 2018 outage demonstrates that “CenturyLink was indisputably aware that TSYS used at least one circuit impacted by the December 2018 outage...”⁹⁵ TSYS also explained that “[t]he vast majority of TSYS circuits are used for 911 services,” a fact which I expect CenturyLink was likely to be aware of

24

25

26

27

⁹³ Webber, Exh. JDW-22C at 2.

⁹⁴ Webber, Exh. JDW-6C at 4-5. *See also*, Webber, Exh. JDW-18C at 1-2.

⁹⁵ Webber, Exh. JDW-22C at 3. *See also*, Webber, Exh. JDW-22C at 5-6.

[REDACTED]

1 as a general matter.⁹⁶ Moreover, TSYS informed CenturyLink during the December
2 2018 outage that these specific circuits were experiencing impairment:

3 In addition, TSYS communicated the specific circuits being utilized to
4 provide interconnection between ESInet 1 and ESInet 2 during the
5 CenturyLink December 2018 outage when TSYS's personnel called
6 CenturyLink's network operations center ("NOC") and reporting that specific
7 DS-1 circuits were experiencing intermittent impairment. Since this
8 information was reported to CenturyLink's NOC during a telephone call,
9 there was no written documentation of TSYS providing such information to
10 CenturyLink during the outage.⁹⁷

11
12 **Q. How does TSYS characterize the impairment of those four SS7 circuits during**
13 **the December 2018 outage?**

14 A. TSYS explained that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

19 [REDACTED]
20 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]⁹⁸

26 [REDACTED]
[REDACTED]⁹⁹

⁹⁶ Webber, Exh. JDW-22C at 3.

⁹⁷ Webber, Exh. JDW-22C at 3.

⁹⁸ Webber, Exh. JDW-19C at 2.

⁹⁹ Webber, Exh. JDW-19C at 2. *See also*, Webber, Exh. JDW-23C at 3 (stating "When one or more circuits were down, SS7 traffic was automatically diverted to the operational one(s). The capacity of each link is enough to handle all SS7 traffic between TNS and TSYS in normal circumstances.").

1 VI. ANALYSIS OF 911 CALLING DATA DURING THE OUTAGE PERIOD

2 A. During the December 2018 outage, nearly [REDACTED] calls made to the
3 Washington E911 system failed to complete, constituting nearly [REDACTED] of
4 the total E911 call volume over that period.

5
6 Q: Did you analyze and estimate the number of Washington E911 calls impacted
7 during the December 2018 outage?

8 A: Yes. As I explain in this section, based upon calling data supplied by CenturyLink in
9 response to Staff discovery, I estimate that a total of [REDACTED] calls made to the
10 Washington E911 system failed to complete during the December 2018 outage. That
11 figure represents some [REDACTED] of the total volume of E911 calls made to the system
12 during that time. The failed calls included [REDACTED] calls bound for TSYS-served
13 PSAPS, and another [REDACTED] calls bound for CenturyLink-served PSAPS. The table
14 below summarizes the call delivery performance of the Washington E911 system
15 during the outage.

16 *Table 1: Impacts of the December 2018 Outage on Washington E911 Calls*

E911 Calls Completed/Failed During the December 2018 Outage				
<i>Data in grey shading is Confidential</i>				
	<u>Completed</u>	<u>Failed</u>	<u>Total</u>	<u>% Failed</u>
Calls to TSYS-Served PSAPs	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Calls to CenturyLink-Served PSAPs	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Total WA E911 System Calls	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: QSI Analysis of CenturyLink Response to Staff DR-20 (9-15-21), Confidl Attach 20(C).

17
18 As I discuss below, however, while CenturyLink and its E911 partner Intrado
19 (formerly named West) are the key sources of this data, Staff has experienced
20 considerable difficulty obtaining through discovery complete and accurate data from

1 CenturyLink concerning these calls, and our investigation on this issue is ongoing.
2 While I believe the call counts provided above reasonably portray the impact of the
3 December 2018 outage on the Washington E911 system, they may be adjusted
4 upward or downward upon review of additional information learned later in this
5 proceeding.

6

7 **Q. Did CenturyLink have the capability to provide Staff with detailed information**
8 **concerning all of the Washington 911 calls that it handled during the December**
9 **2018 outage?**

10 A. Yes. Telecommunications services providers routinely generate call detail records
11 (“CDRs”) for every call in the course of processing calls traversing their networks.
12 CDRs are automatically-generated records produced at a point of switching that
13 capture the details of a received or transmitted call and become stored in a
14 database.¹⁰⁰ In this case, the points of switching where the CDRs for Washington 911
15 calls were generated were the selective routers numbers 1 and 2 of CenturyLink’s
16 ESInet I partner company, Intrado (formerly named West Telecom Services).¹⁰¹
17 Given that CenturyLink ultimately produced those CDRs in September 2021 in
18 response to persistent follow-up discovery from Staff, it is clear that Intrado
19 generated and stored CDRs for the December 2018 outage period, and that
20 CenturyLink could have easily requested and obtained them from Intrado/West at
21 any time after the event.

¹⁰⁰ Webber, Exh. JDW-9 at 5.

¹⁰¹ As explained in Staff’s Investigation Report, West Telecom Services, LLC changed its name to Intrado Communications, LLC with the Commission effective May 1, 2020. Webber, Exh. JDW-3C at 5, fn. 5.

1 **Q. During Staff’s initial investigation of the December 2018 incident, did Staff**
2 **attempt to obtain those CDRs from CenturyLink?**

3 A. Yes. As described in its Investigation Report, Staff asked CenturyLink on four
4 separate occasions to specify the number of Washington customers impacted by the
5 December 2018 outage. The first three times, CenturyLink refused to provide that
6 information because it claimed that no services under the Commission’s jurisdiction,
7 including E911 service, were impacted by the outage.¹⁰² Staff’s Report then cited to
8 CenturyLink’s Response to Staff DR CP 2, dated September 18, 2020, as finally
9 providing data on all E911 emergency calls that CenturyLink was to deliver to TSYS
10 during the December 2018 outage.¹⁰³

11 However, Staff also served discovery on CenturyLink in August 2019 seeking those
12 CDRs. Regulatory Staff data requests RS-7 and RS-8 sought:

- 13 • RS-7: “all call logs and call detail recording (CDR) information on all 911
14 calls that were completed to WA State PSAPs still under CenturyLink’s
15 management during the Dec. 27 – Dec. 28, 2018 911 outage.” And
- 16 • RS-8: “all call logs and call detail recording (CDR) information on all failed
17 911 calls into Washington PSAPs which traversed CenturyLink’s
18 infrastructure during the Dec. 27 – Dec. 28, 2018 911 outage.”

19 In September 2019, CenturyLink provided separate spreadsheet (Excel®) files in
20 response to each of those requests.¹⁰⁴ I understand from my discussions with
21 Rebecca Beaton (Commission telecom regulatory analyst) that Staff and its
22 consultant at that time reviewed these CDR datasets and concluded that they
23 appeared to contain errors and record omissions, which in fact CenturyLink

¹⁰² Webber, Exh. JDW-24.

¹⁰³ Webber, Exh. JDW-3C at 13.

¹⁰⁴ Webber, Exh. JDW-25; Webber, Exh. JDW-26C.

1 subsequently admitted (see discussion below). For that reason, Staff did not rely
2 upon those data responses when first evaluating the volume of failed 911 calls at the
3 time that it prepared its Investigative Report.

4
5 **Q. Did you analyze 911 call data recorded during the December 2018 outage to**
6 **estimate how many calls were successfully delivered to Washington PSAPs**
7 **during that period, and how many calls failed to be delivered?**

8 A. Yes. I reviewed all of the Washington 911 call CDR data and related summary
9 information that CenturyLink provided to Staff to date since the December 2018
10 incident, including the Company's responses to RS-7 and RS-8 in 2019, to data
11 requests CP-1¹⁰⁵ and CP-2¹⁰⁶ in 2020, and to Staff DRs 20-22 in 2021.¹⁰⁷

12 When comparing CenturyLink's 2019 and 2020 data request responses, I
13 found several significant discrepancies between CDR data supplied in 2019
14 (specifically, in the RS-8 Confidential Attachment B spreadsheet) and the calls
15 summary provided in 2020, Attachment DR-2 to the CP-2 response.¹⁰⁸ But instead of
16 rebutting or explaining those discrepancies, CenturyLink's Response to Staff DR-22
17 admitted (after first stating an objection to the request) that the RS-8 Confidential
18 Attachment B spreadsheet was missing data and that the Company could neither
19 explain why nor replicate that spreadsheet:

¹⁰⁵ Webber, Exh. JDW-27C (requesting "all call recording details for all emergency services calls that CenturyLink processed for the PSAPs it still 'owned' in Washington state during the outage period...."); Webber, Exh. JDW-28C.

¹⁰⁶ Webber, Exh. JDW-29C (requesting "[a] detailed report providing information on all emergency calls, received by CenturyLink, that were ultimately destined for Comtech's PSAPs in Washington state...." during the outage period); Webber, Exh. JDW-30C.

¹⁰⁷ Webber, Exh. JDW-6C; Webber, Exh. JDW-31C.

¹⁰⁸ See Webber, Exh. JDW-6C at 11.

1 It appears that the file provided in September 2019 was inadvertently
2 missing data. Because the file was produced 2 years ago, and because there
3 has been no follow-up by Staff since that time, CLC is not clear as to how
4 the errors occurred, and is unable to replicate the September 2019
5 spreadsheet.¹⁰⁹

6 CenturyLink then supplied an entirely new spreadsheet on September 15, 2021,
7 “Confidential Attachment Staff 20,” that it claims contains selected E911 CDR
8 information “for December 27-29, 2018...[that] includes all Washington data, and is
9 not isolated for PSAPs served (at the time) by CenturyLink or Comtech.”¹¹⁰ Given
10 CenturyLink’s repudiation of the CDR data it had previously provided, I have relied
11 only on this new spreadsheet going forward, with the caveat that as an independent
12 third party, I am not in a position to confirm that the new spreadsheet is error-free
13 and contains accurate records for all of the Washington E911 calls that traversed
14 CenturyLink’s ESInet I network during the outage period.¹¹¹

15
16 **Q. Mr. Webber, have you been able to analyze the E911 call data supplied in**
17 **CenturyLink’s Confidential Attachment Staff 20 to estimate how many calls**
18 **were completed (successfully delivered to Washington PSAPs) during the**
19 **outage period, and how many calls failed?**

20 **A. Yes.** As I explained above, CenturyLink indicated that its Confidential Attachment
21 Staff 20 (hereafter referred to as the “Staff DR-20” spreadsheet or data) provides call

¹⁰⁹ Webber, Exh. JDW-6C at 11.

¹¹⁰ Webber, Exh. JDW-6C at 9; Webber, Exh. JDW-31C.

¹¹¹ However, I did compare the call counts for Confidential Attachment Staff 20 to those supplied in Attachment DR-2 to the CP-2 response from September 2019, and found they are in good agreement, for calls destined to TSYs-served PSAPs. The two data sources have the same timespan; and while there are some discrepancies in the call counts they generally are small: Comparing DR2 vs. Staff 20C by category I found:

[REDACTED]

Compare, Webber, Exh. JDW-30C with, Webber, Exh. JDW-31C.

1 records for all 911 calls to Washington PSAPs during the December 2018 outage.

2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED].¹¹²

8 **Q. What criteria did you apply to categorize a call as completed or failed?**

9 A. I analyzed this data by (a) creating extracts of the date and starting time for each call,
10 so that they can be categorized into distinct hour bands for each day December 27-29
11 (e.g., 8am-8:59am, 9am-9:59am, etc.); (b) segregating those calls destined to PSAPs
12 served by TSYS vs. those still served by CenturyLink; and (c) distinguishing
13 between calls with the [REDACTED]

14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED].

18
19 **Q. Did you find that some calls marked as [REDACTED] may not have been**
20 **successfully completed?**

21 A. Yes, as stated above. [REDACTED]
22 [REDACTED]

¹¹² Webber, Exh. JDW-31C.

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

6

7 **Q. Have you counted those additional calls as “failed” in your analysis?**

8 A. No, at this point I have not. To be conservative I have refrained from classifying
9 those calls as “failed” unless/until further data comes to light that confirms they
10 should be classified in that manner. Our investigation is continuing on this issue and
11 certain other calls destined for CenturyLink-served PSAPs, as I describe later in my
12 testimony.

13

14 **Q. What timespan did you apply when conducting your analysis of completed vs.
15 failed calls?**

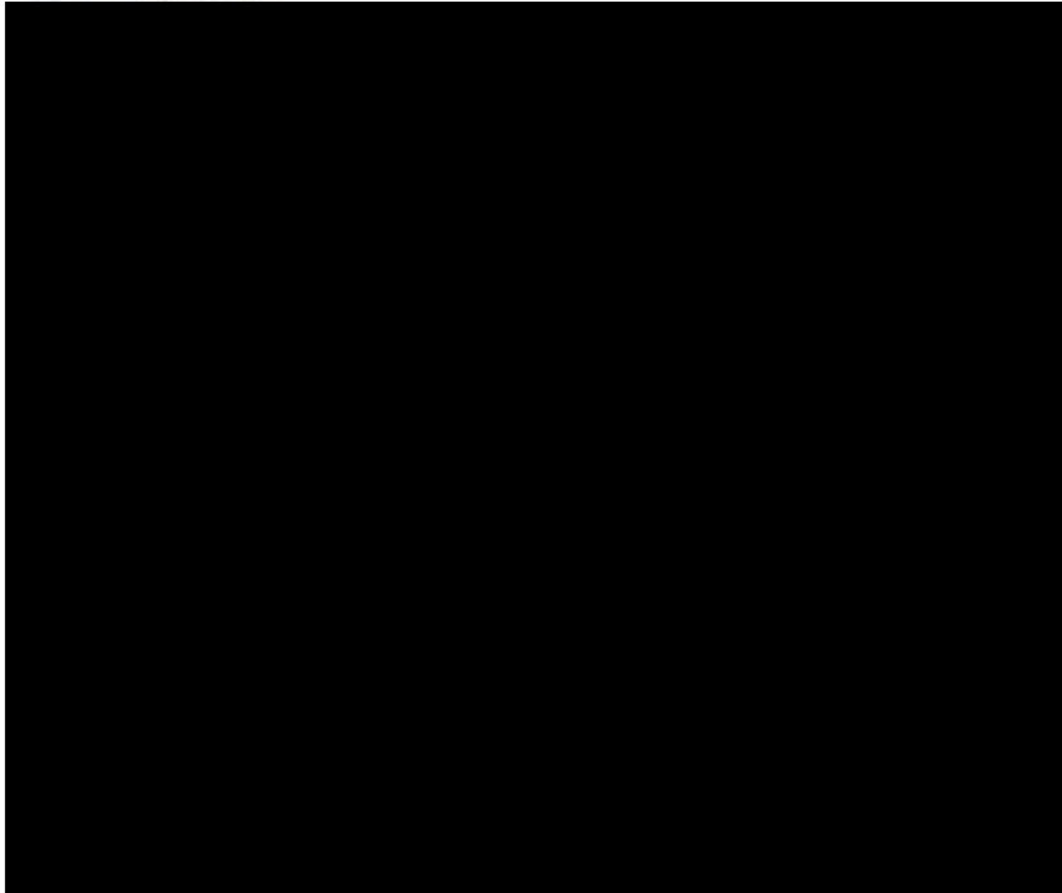
16 A. I applied the timespan that Staff had previously used when evaluating the impacts of
17 the outage, namely a duration of 49 hours and 32 minutes, starting at 12:40 a.m.
18 Pacific Standard Time (“PST”) on December 27, 2018.¹¹³ For Washington E911
19 services, the outage’s impacts were not uniform but varied over time and by whether
20 a PSAP was connected to and served by CenturyLink or TSYS, with the PSAPs that
21 had been transitioned to ESInet II (TSYS) suffering the most severe impacts.

22

¹¹³ Webber, Exh. JDW-3C at 4.

1 **Q. How has TSYS characterized the impact of the outage on its system, ESInet II?**

2 A. TSYS described the impact of the outage in its initial Major Outage Report:¹¹⁴



3

4 **Q. What was the overall impact of the outage on E911 calls destined to Washington**
5 **PSAPs during the outage?**

6 A. Figure 2 below provides an overview of the outage's impact on the Washington
7 E911 system. Based on the DR-20 data supplied by CenturyLink, this chart gives the
8 counts of E911 calls by hour band, [REDACTED]

■ [REDACTED]

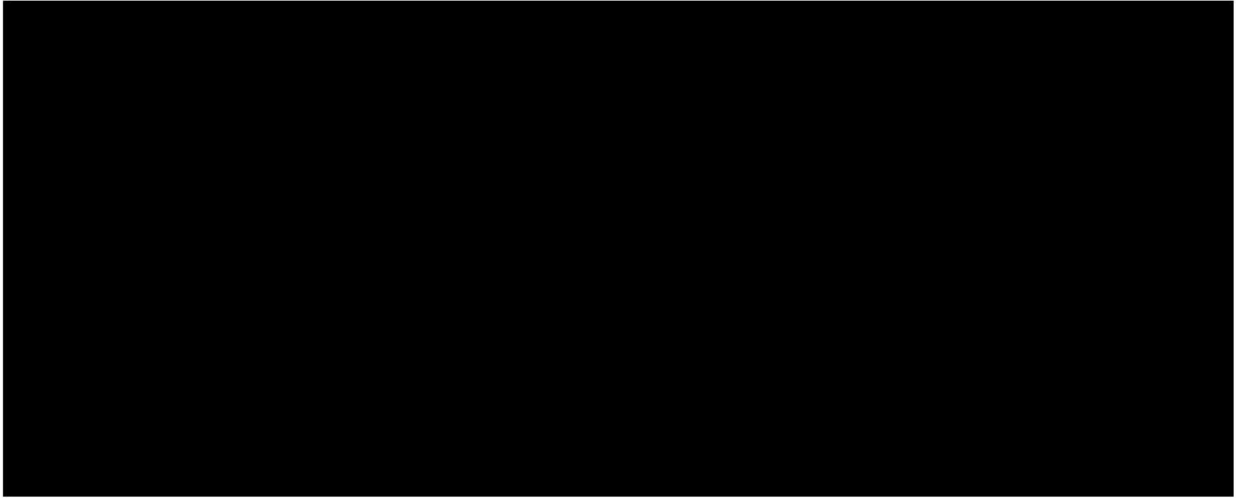
¹¹⁴ Webber, Exh. JDW-32C.

1

2

3

Figure 7: Chart of E911 Call Counts During the December 2018 Outage



4

5

6

Q. What was the impact on calls destined to PSAPs served by TSYS?

7

8

A. Table 2 below provides the call counts during the outage for the 47 PSAPs served by

9

TSYS. According to CenturyLink's DR-20 data, during the 49 hour, 32 minute

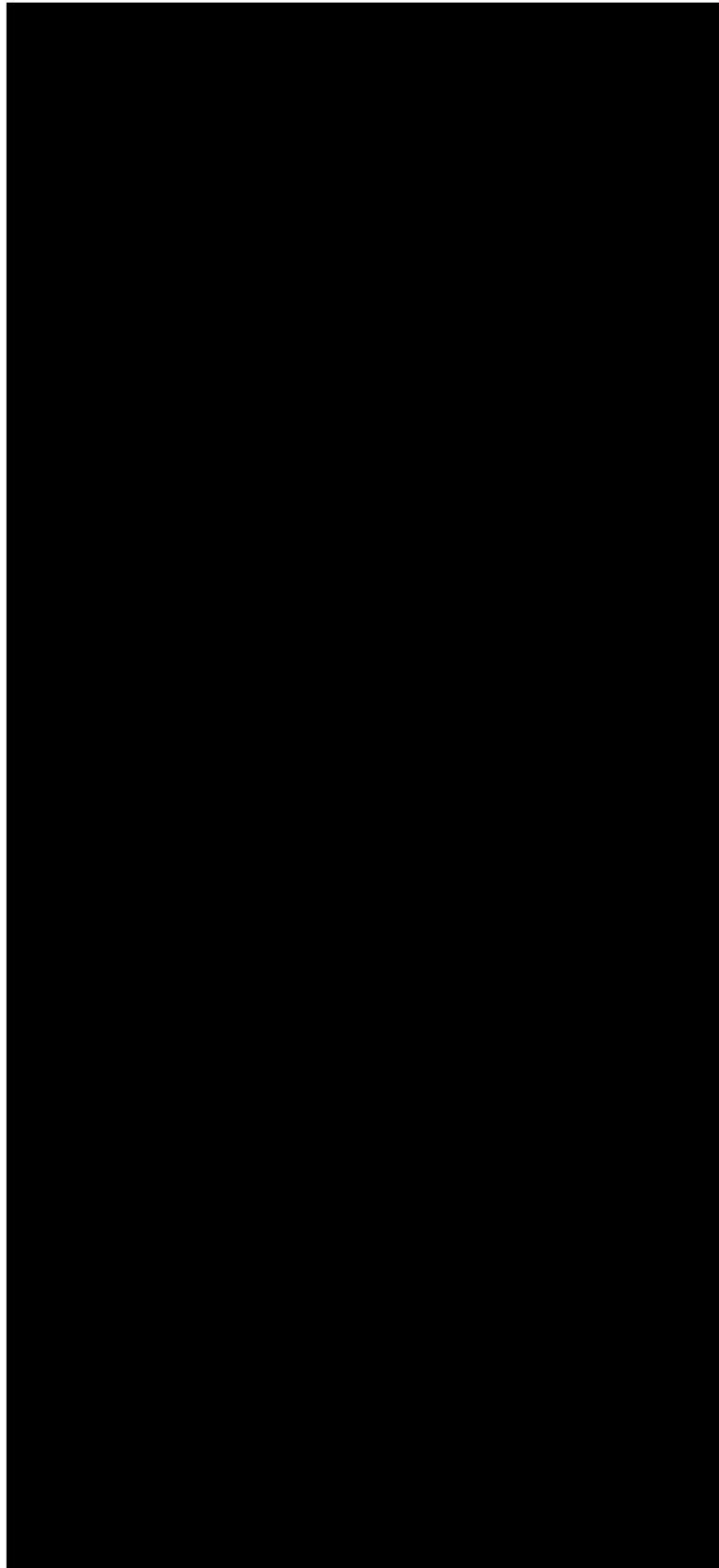
10

outage span

11

12

Table 2: E911 Call Counts, for TSYs-Served PSAPs



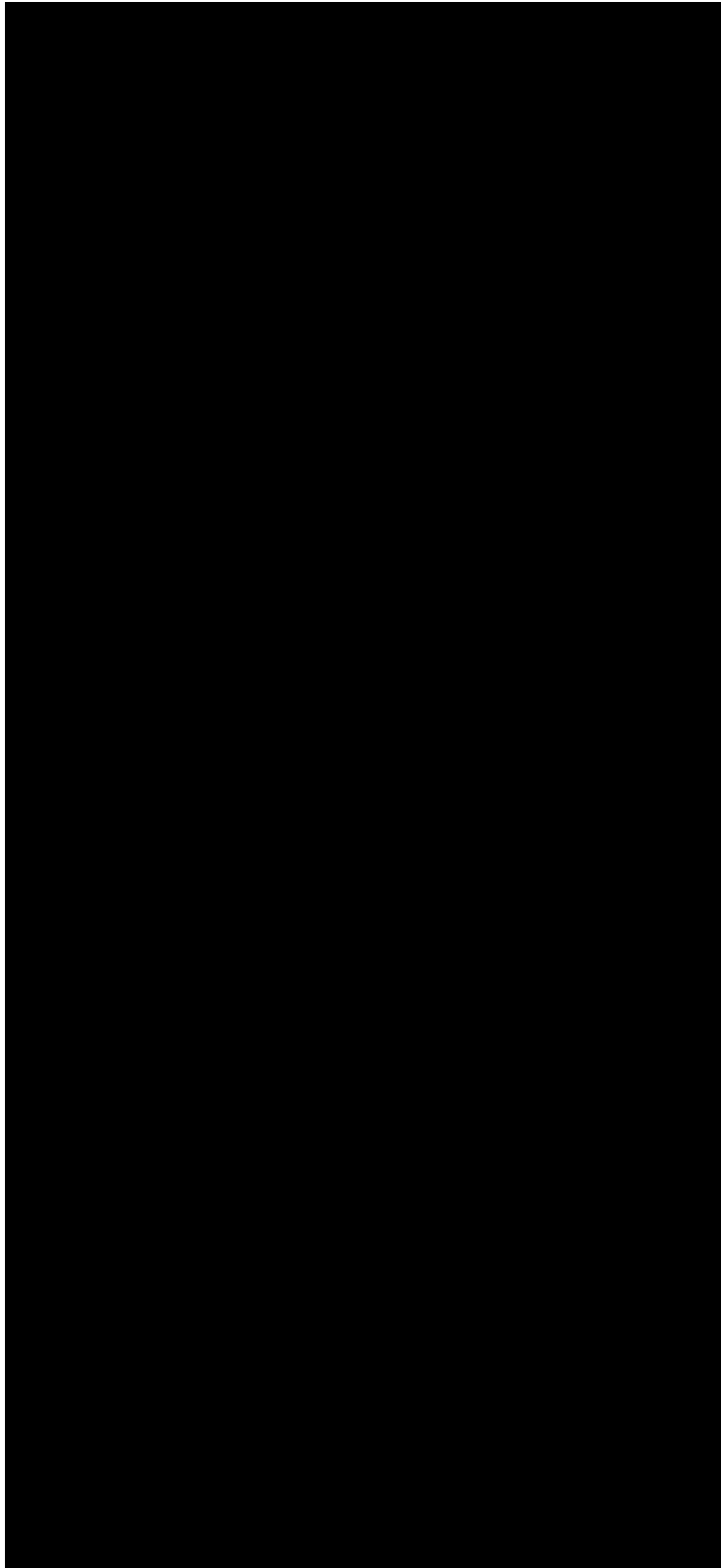
1 **Q. And what was the impact on calls destined to PSAPs served by CenturyLink?**

2 A. Table 3 below provides the call counts during the outage for the 15 PSAPs that were

3 still served directly by CenturyLink over its ESInet I.

4

Table 3: E911 Call Counts, for CenturyLink-Served PSAPs



1 CenturyLink's data indicates that [REDACTED] E911 calls were destined to the PSAPs it
2 continued to service directly, of which [REDACTED] failed.

3

4 **Q. Did you conduct further analysis of the second time period identified in TSYS's**
5 **Major Outage Report??**

6 A. Yes. The second time period that TSYS identified as a time when [REDACTED]

7 [REDACTED] The
8 following charts and tables focus on the period ("Period 2") to better elucidate the
9 severity of the outage on Washington's E911 services.

10 The figure and table below show the Period 2 impacts on calls destined to
11 TSYS-served PSAPs. As they illustrate, [REDACTED]

12 [REDACTED]

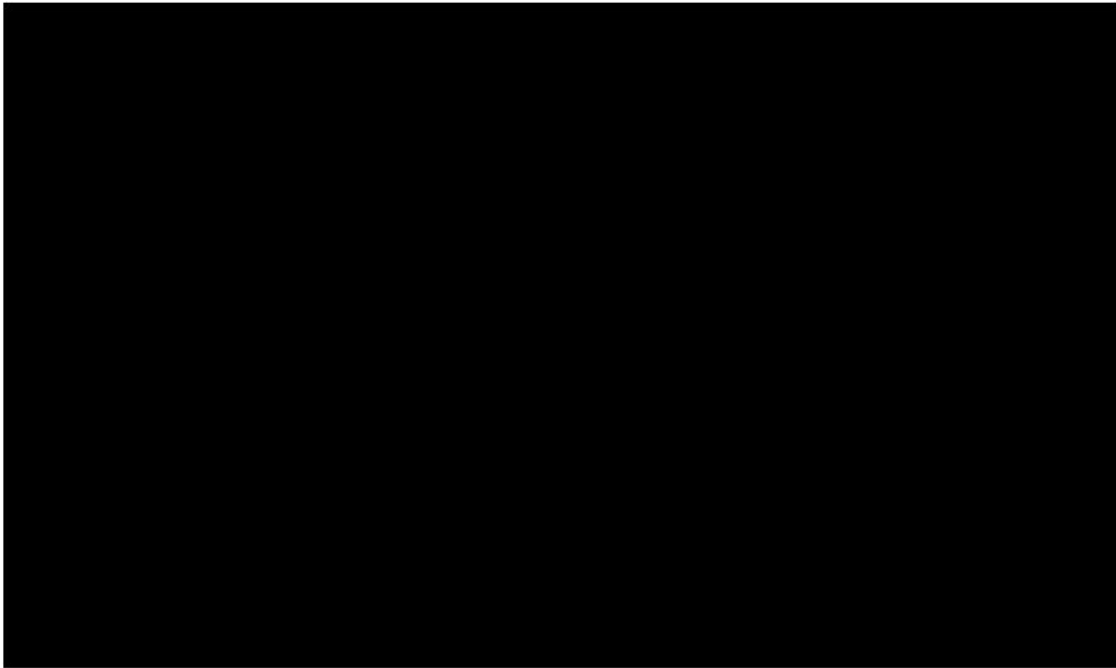
13 [REDACTED]

14 [REDACTED].

15

1

Figure 8: Period 2 Impacts on Calls to TSYs-Served PSAPs



2

3

Table 4: Period 2 Impacts on Calls to TSYs-Served PSAPs

A large black rectangular redaction box covering the entire content of Table 4.

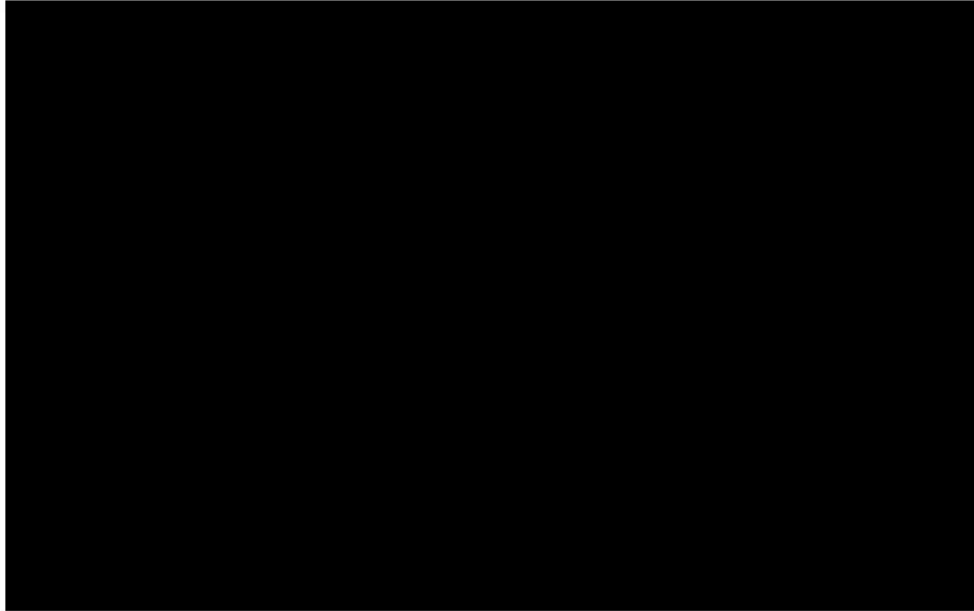
4

5 And the figure and table below present parallel data for the 15 PSAPs served by

6 CenturyLink at the time of the outages:

1

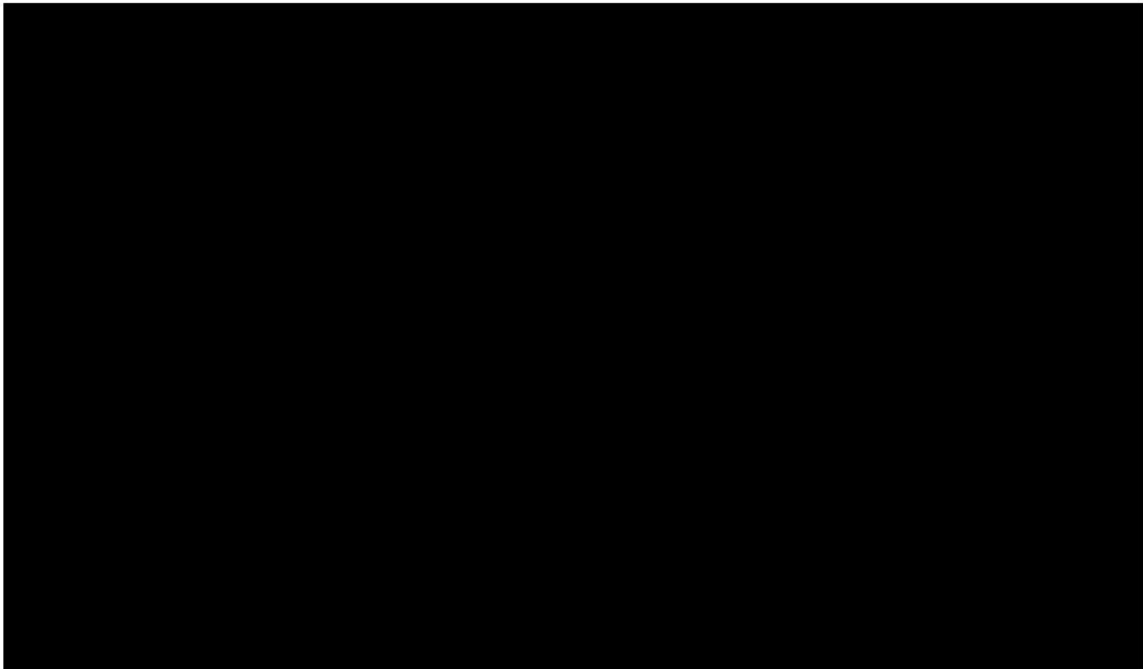
Figure 9: Period 2 Impacts on Calls to CenturyLink-Served PSAPs



2


3

Table 5: Period 2 Impacts on Calls to CenturyLink-Served PSAPs



4

5 **Q. What conclusions do you draw from this analysis?**

6 A. First, the data presented above indicates that the outage during Period 2 greatly
7 impacted TSYs-served PSAPs, with 

1 [REDACTED]
2 [REDACTED] – which conflicts with the characterization in the TSYS Major Outage
3 Report that [REDACTED] were being received during that time. Second, this data shows
4 that [REDACTED]

5 [REDACTED], which appears contrary to CenturyLink’s
6 assertions that it experienced no incident-related outages on its Washington E911
7 network.¹¹⁵

8

9 **Q. What did you learn about the failed calls experienced by CenturyLink-served**
10 **PSAPs during Period 2?**

11 A. I learned that the majority of those failed calls were directed to two PSAPs that were
12 still served directly by CenturyLink at that time, namely [REDACTED]

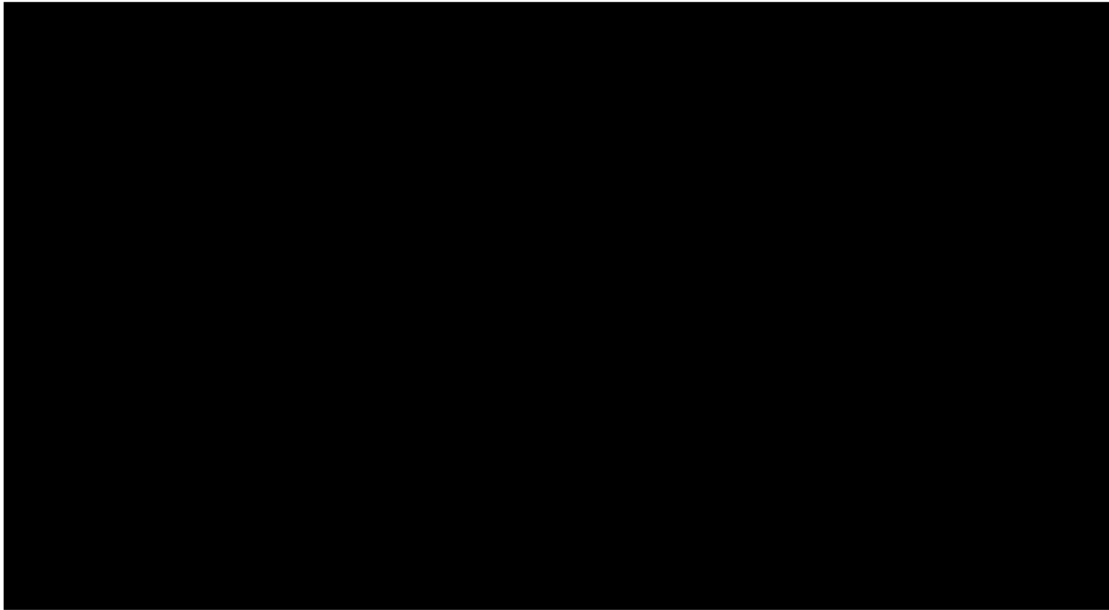
13 [REDACTED] Over the entire incident
14 time frame, CenturyLink’s calling data indicates that these two PSAPs experienced
15 [REDACTED] and [REDACTED] failed 911 calls, respectively (about [REDACTED] of their total 911 calls over
16 that time span). While there appears to be a strong correlation with the [REDACTED]
17 [REDACTED] outage, as shown in the chart below, it is not clear why those two PSAPs
18 experienced that level of failed calls, while other PSAPs served by ESInet I did not.

19

¹¹⁵ Webber, Exh. JDW-24 at 5 (stating, “[CenturyLink] **Response:** No CenturyLink services under the WUTC’s jurisdiction, including CenturyLink’s 911 service, were affected.”); (responding that none of the Washington 911 calls to the CenturyLink served PSAPs failed to complete).

1
2

Figure 10: Failed Calls During Period 2 for [REDACTED] Served by CenturyLink



3

4

Figure 10 compares the failed call counts trends for the two [REDACTED] with the trend for all PSAPs, with the latter scaled downward by a factor of 100 (i.e., total PSAPs failed calls ÷ 100) to facilitate comparison of their overall trends. There clearly appears to be a strong correlation, but CenturyLink failed to provide the reasons why the two [REDACTED] experienced the failed calls shown above. We continue to investigate the possible causes of these failed calls.

5

6

7

8

9

10

11 **Q. Does this conclude your Direct Testimony?**

12 **A. Yes.**