

Exhibit O

Redacted Version

**BEFORE THE WASHINGTON
UTILITIES & TRANSPORTATION COMMISSION**

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

Complainant,

v.

CENTURYLINK COMMUNICATIONS, LLC, et al.,

Respondents.

DOCKET UT-181051

**CROSS-ANSWERING TESTIMONY OF BRIAN ROSEN
ON BEHALF OF
WASHINGTON STATE OFFICE OF THE ATTORNEY GENERAL
PUBLIC COUNSEL UNIT**

Exhibit BR-30CT

August 31, 2022

**Shaded Information is Designated Confidential
per Protective Order in Docket UT-181051**

**CROSS-ANSWERING TESTIMONY OF BRIAN ROSEN
EXHIBIT BR-30CT
DOCKET UT-181051**

TABLE OF CONTENTS

I. INTRODUCTION / OVERVIEW..... 1

II. TECHNOLOGY CHOICES 2

III. DIVERSITY 8

IV. TRANSITION RESPONSIBILITIES 19

V. FAILURES IN THE GREEN NETWORK..... 29

VI. CONCLUSIONS..... 31

FIGURES

Figure 1 - Trust IP Interconnect..... 28

Figure 2 - Untrusted IP Based Interconnect..... 28

Figure 3 - SS-7 Based Interconnect 28

**CROSS-ANSWERING TESTIMONY OF BRIAN ROSEN
EXHIBIT BR-30CT
DOCKET UT-181051**

EXHIBITS LIST

- | | |
|----------------|---|
| Exhibit BR-31 | Public Counsel Response to CenturyLink Data Request No. 17 with Attachments |
| Exhibit BR-32C | Comtech Response to Public Counsel Data Request No. 31 with Confidential Attachment |

I. INTRODUCTION / OVERVIEW

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

2 A. My name is Brian Rosen and my business address is 470 Conrad Drive, Mars,
3 Pennsylvania 16046. I am the principal consultant for Brian Rosen Technologies
4 LLC, where I provide guidance to states and local governments on deployment of
5 Next Generation 9-1-1 (NG9-1-1) systems.

6 **Q. On whose behalf are you testifying?**

7 A. I am testifying on behalf of the Public Counsel Unit of the Washington Attorney
8 General's Office (Public Counsel).

9 **Q. Have you previously provided testimony in this proceeding?**

10 A. Yes, I provided testimony for Public Counsel Unit of the Washington State Attorney
11 General's Office (Public Counsel).

12 **Q. What exhibits are you sponsoring in this proceeding?**

13 A. I am sponsoring the following exhibits:

14 Exhibit BR-31 Public Counsel Response to CenturyLink Data Request No. 17
15 with Attachments

16 Exhibit BR-32C Comtech Response to Public Counsel Data Request No. 31
17 with Confidential Attachment

18 **Q. What is the purpose of your cross-answering testimony?**

19 A. In this testimony, I respond to CenturyLink witness testimony with regard to
20 technology choices, diversity, transition responsibilities and Green Network failure.

II. TECHNOLOGY CHOICES

1 **Q. Refer to Exhibit SET-1TC at 8:17–18. CenturyLink witness Steven E. Turner**
2 **states: “SS7 technology is commonly used by the industry in 911 network**
3 **architecture.” Is this true?**

4 A. Yes, however Signaling System 7 (SS7) is not commonly used in Next Generation
5 9-1-1 (NG9-1-1) systems other than in the originating service provider (OSP)
6 interconnect. SS7 was used in the older E9-1-1 system in two places: connecting to
7 some originating service providers and in tandem-to-tandem connections where
8 multiple selective routers were interconnected. In some NG9-1-1 systems, SS7 is still
9 used to connect OSPs to NG9-1-1 because those OSPs have not converted to Session
10 Initiation Protocol (SIP), not because SS7 is superior technology.

11 **Q. At the time of the outage, was the Washington 9-1-1 system an older E9-1-1**
12 **system you just described?**

13 A. No. At the time of the outage, the Washington 9-1-1 system was transitioning from an
14 early, IP-based service, which was a migration step to a standards-based NG9-1-1
15 system. For the CenturyLink system, which was established prior to the NG9-1-1
16 standards, the contract states: “To accomplish this, there must be a switch from the
17 antiquated legacy analog telephone system to a system as used in cellular and
18 computer voice over internet (VoIP) protocols by telephone and communication

1 providers.”¹ CenturyLink’s network (ESInet 1) and Comtech’s network (ESInet 2)
2 were both IP networks.

3 **Q. Is it common in the industry to use an SS7 interconnect between two IP**
4 **networks?**

5 A. No. Using an SS7 interconnect between two IP networks is highly unusual.

6 **Q. Based upon your review of the record, did CenturyLink and Comtech discuss**
7 **other options for interconnecting the two IP networks?**

8 A. Yes. Emails in the record² make clear that Comtech attempted to get CenturyLink to
9 use an IP interconnect that closely resembles the current NG9-1-1 standards for
10 interconnecting ESInets. Comtech’s proposal used SIP signaling which adhered
11 closely to SIP signaling used within a standards-based NG9-1-1 system.³ While the
12 current NG9-1-1 standards were published after the outage at issue here, the
13 similarity to the standards shows that Comtech’s IP interconnect proposal was
14 reasonable.

15 Although the details remain unclear, it appears that CenturyLink proposed an
16 IP interconnect that was quite different from what Comtech (and the eventual NG9-1-
17 1 standards) described. CenturyLink proposed to use protocols that are not used in
18 NG9-1-1 systems. Based upon my professional experience, it appears to me that
19 Comtech offered a reasonable proposal, closely aligned to NG9-1-1 standard, while

¹ Brian Rosen, Exh. BR-4C at 15 (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196 at 14).

² See Rosen, Exh. BR-18C (Comtech Response to Public Counsel Data Request No. 4 with Confidential Attachment B.1(b)).

³ Nat’l Emergency Number Ass’n (NENA), *NENA i3 Standard for Next Generation 9-1-1* (2021), https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-010.3b-2021_i3_stan.pdf.

1 CenturyLink countered with an IP interconnect at odds with those standards.

2 CenturyLink also told Comtech that it could use SS7 to interconnect.

3 Faced with the available choices from CenturyLink, Comtech preferred the
4 SS7 interconnect. CenturyLink and Comtech went ahead and implemented the SS7
5 interconnect.

6 **Q. Refer to Exhibit SET-1TC at 8 and 58 and Exhibit CDK-1TC at 12–13.**

7 **CenturyLink’s witnesses insist SS7 was an appropriate technology choice for the**
8 **interconnect. Why was SS7 inappropriate for this use case?**

9 A. SS7 was inappropriate for this use case because it introduced unnecessary complexity
10 and additional opportunity for failure into the state’s critical 9-1-1 system with less
11 ability for the system to quickly recover from failures. At the time of this migration,
12 the OSPs were still connected to the CenturyLink ESInet by the older Centralized
13 Automatic Message Accounting (CAMA) technology, and the Public Safety
14 Answering Points (PSAPs) were also connected using older CAMA technology. This
15 meant that there was interwork between the SS7 or CAMA connections from the OSP
16 to the CenturyLink ESInet, and another conversion between the ESInet and the
17 CAMA connections to the PSAPs. The choice of using SS7 for the interconnect
18 meant two additional conversions (IP to SS7 and SS7 to IP) were introduced into the
19 system. This resulted in a total of **four conversions** for every call destined for a
20 transitioned PSAP.

21 Every transition adds complexity and the opportunity to introduce failure into
22 the system. Furthermore, SS7 has a known weakness, which is that designers have to

1 anticipate all possible failures and engineer backup paths into the system expressly. In
2 contrast, IP networks have the very desirable characteristic that they automatically
3 discover backup paths and use them, regardless of how circuitous or complex the path
4 is, if that is the only way to get from point A to point B.

5 In extreme failure conditions, IP networks are more likely to work compared
6 to SS7 networks. Indeed, there were IP connections between the contractors
7 providing location information for calls (Automatic Location Identification query),⁴
8 and they worked throughout the incident. NG9-1-1 is being deployed across the
9 country for this reason, among others, and to my knowledge, no new 9-1-1 systems
10 use SS7 except for connections to originating service providers who have not
11 converted to SIP.

12 **Q. Was there anything else unusual about this SS7 interconnect?**

13 A. Yes. In addition to lack of diversity, which I will discuss later in my testimony,
14 CenturyLink instructed Comtech to use a third party, Transaction Network Services
15 (TNS), to provide the actual SS7 interconnect between its contractor (Intrado) and
16 Comtech.⁵

17 Both Intrado and Comtech had relationships with TNS prior to this
18 interconnect. TNS is a commercial supplier of SS7 interconnect. It is not a carrier,
19 and does not offer or claim to offer 9-1-1 capability. Its network is not subject to
20 diversity requirements, and it does not claim to offer audited diverse paths within its

⁴ Rosen, Exh. BR-29C (Comtech Response to Public Counsel Data Request No. 9).

⁵ Rosen, Exh. BR-18C at 1.

1 network as 9-1-1 providers are required to do.

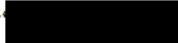
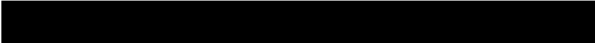
2 **Q. Refer to Carl Klein’s Exhibit CDK-1TC at 12–13 and Exhibit SET-1TC at 44–**
3 **45. CenturyLink witnesses Klein and Turner object to your characterization of**
4 **SS7 as obsolete. Do you agree with these objections?**

5 A. No. SS7 is being phased out all over the country in favor of SIP, the signaling
6 protocol used in NG911, as well as wireless networks, Voice over Internet Protocol
7 (VoIP) networks, and enterprise networks. SIP is replacing SS7, as well as the other
8 signaling for telephone calls, as it was originally designed to do. I have been involved
9 with the development of SIP since its inception, and I know well that SS7 is phasing
10 out and SIP is becoming dominant.

11 Wireless networks have almost completely phased out SS7, the remaining SS7
12 are almost all confined to interfaces to non-wireless carriers. Larger telephone carriers
13 are phasing out SS7 within their networks, especially at interconnects between service
14 providers. Through discussions with other industry professionals, it is my
15 understanding that carriers have asked the Federal Communications Commission
16 (FCC) to allow them to only allow SIP interconnect and not support SS7 interconnect
17 with other carriers, but the FCC has not issued an order addressing this issue.⁶

18 Moreover, many SS7 vendors have left the business, and usage has been
19 declining for a long time. A significant problem in older SS7 networks is that the

⁶ See generally *Technology Transitions*, GN Docket No. 13-5, 28 FCC Rcd. 105 (issued Jan. 10, 2013) and *AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition*, GN Docket No. 12-353, 27 FCC Rcd. 15766 (issued Dec. 14, 2012).

1 vendor who supplied the equipment is no longer supporting it. While there is some
2 truth to the statement “it is used to support every 911 network”⁷ and “
3 ,”⁸ SS7 must be used to connect certain
4 carriers, such as CenturyLink and other wireline carriers, who have so far refused to
5 convert their 9-1-1 calls to SIP. Thus, the older, obsolete technology has to be used
6 until these carriers are forced to modernize their 9-1-1 support. However, SS7 is not
7 used in the middle of an NG9-1-1 network. It is only at the edge of the network facing
8 OSPs that have refused to deliver 9-1-1 calls via SIP. Turner’s testimony confirms
9 this.⁹

10 In addition, SS7 does not support location in 9-1-1, even in older systems.
11 Location information in E9-1-1 is supplied over dedicated trunks using the Automatic
12 Location Identification (ALI) database. When OSPs connect via SS7 to NG9-1-1
13 systems, location comes from a simulated ALI over IP or directly over IP from a
14 database. SS7 has no facility to support location transmission.

15 Finally, this failure shows why SS7 is inherently less reliable than IP. There
16 were only four links, and they all had to be engineered point to point over dedicated
17 circuits. By contrast, IP networks have many more connections, direct and indirect.
18 When engineered in the way Comtech proposed, an IP network would have provided
19 much more tolerance for failures. Specifically, when connecting these two IP
20 networks via IP, there would not have been any dedicated long-distance links.

⁷ Response Testimony of Carl D. Klein, Exh. CDK-1TC at 12:15–16.

⁸ Response Testimony of Steven Turner, Exh. SET-1TC at 45:3.

⁹ *Id.* at 45:12–20.

1 Instead, the system would likely have used a mix of Virtual Private Network
2 connections over public Internet, Multiprotocol Label Switching (or similar)
3 connections, and direct ties at common colocation facilities. Notably, the IP network
4 connections between Intrado and Comtech worked during this failure as did the IP-
5 based ALI connections between CenturyLink and Comtech.¹⁰

III. DIVERSITY

6 **Q. Refer to Martin Valence’s Exhibit MDV-1TC at 5–10 and Exhibit SET-1TC at**
7 **57–58. CenturyLink’s witnesses cite lack of diversity on Comtech’s part as the**
8 **cause of the outage. Please explain diversity and how it applies to the incident.**

9 A. The term “diversity” is used to describe how a network is designed to avoid common
10 faults. Circuits fail, for a variety of reasons. For example, cables get cut by
11 construction, weather events occur, electronics fail, or people make mistakes. In an
12 SS7 network, there are signaling paths and “trunks”. The signaling path is used to
13 provide instructions on how to set up connections. The trunks carry the actual call
14 (the “voice path”). The term SS7 generally refers to signaling. By contrast, IP
15 networks have only one mechanism, and the signaling and voice path run on the same
16 network.

17 SS7 networks are constructed of “links” that connect telephone switches and
18 special purpose Signaling Transfer Points (STPs) to each other. An origination
19 network switch will signal a request for a connection, which typically would go to its

¹⁰ Rosen, Exh. BR-29C.

1 local STP. The local STP would connect to other STPs, which relay the request to the
2 destination network STP. The destination network STP then instructs the termination
3 switch to set up the call.

4 These signaling requests transit the “links”. Each link is a circuit, ordered
5 from a service provider. To be reliable, there is more than one link between switches
6 and STPs and between the STPs. Most commonly, STPs are provisioned in pairs, and
7 each member of the pair has two links to each of its partner STP. If any link works
8 (one of the four in the example), then that part of the SS7 signaling network can do its
9 job. If all four links fail, the SS7 network will be unable to complete calls.

10 Recommended SS7 network design requires that the links be diverse.

11 The primary diversity criteria is “geographic” or “geospatial” diversity. This
12 means that the physical path the link takes does not have anything in common with
13 other paths. For example, separate fibers in separate conduits should be sufficiently
14 spaced so a single backhoe incident (e.g., severing a cable) does not disrupt more than
15 one link in the set. It also means separate switches are in the path of the link, so a
16 failure of a single switch does not take all four links down. Geographic diversity was
17 not a factor in this incident.

18 “Network diversity” is another form of diversity applicable to highly available
19 systems like 9-1-1. An entire network will sometimes encounter a problem that takes
20 the whole network down. For example, in this outage the entire optical network went
21 down, and since there was not network diversity, the interconnect failed.

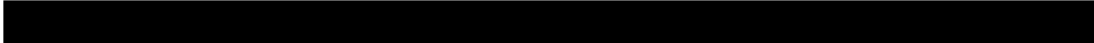
22 “Software diversity” is a third form of diversity. By far, the most common

1 reason for an entire network to fail is a defect or bug in the software from which the
2 network components are built. In most deployed networks today, all the switches or
3 routers are from one company and have common code. This is a “single point of
4 failure” that can affect the entire network.

5 Software is usually continuously maintained while being used in active
6 networks: problems are found and fixed, new capabilities are added, and obsolete
7 capabilities are removed. Software is released in “versions” and most commonly, one
8 network has one software version running in all of its switches or routers. It is
9 possible, as it was in this case, that a bug only affects some versions of software but
10 not others. Experience shows that serious bugs can occur in one version or many
11 versions, and it is not predictable what happens in any brand of switch or specific
12 network.

13 **Q. Refer to Exhibit MDV-1TC at 5–10 and Exhibit SET-1TC at 27–28, 46, 57–58.**
14 **Turner and Valence discuss “supplier diversity”. What is supplier diversity?**

15 **A.** Supplier diversity is having more than one supplier of a network component. To a
16 customer like Comtech, supplier diversity means getting circuits from more than one
17 carrier. Valence claims that because CenturyLink has more than one network, it can
18 offer supplier diversity.¹¹ In my opinion, that is not supplier diversity. Rather, in this
19 context, supplier diversity would be using multiple vendors for circuits. For example,

20 

¹¹ Response Testimony of Martin Valence, Exh. MDV-1TC at 4:6–16.

1 [REDACTED].¹²

2 **Q. How is software diversity different from supplier diversity?**

3 A. Software diversity is diversity of software within a network. Since the root of most
4 modern total network failures is software failure, professionally, I recommend using
5 components that do not all rely on the same software. CenturyLink does not appear to
6 provide software diversity.

7 While the failure only occurred on one of its networks, another network using
8 the same vendor, experienced a separate, but similar failure. CenturyLink claims the
9 versions of the software were different, and the failures that occurred on one network
10 could not have occurred on the other. I find that at least debatable, but without testing
11 and the ability to reproduce the failure, we do not really know. Sometimes, a carrier
12 like CenturyLink will use supplier diversity (meaning, it uses more than one vendor)
13 as equivalent to software diversity, because usually vendors write their own software.
14 I prefer expressing it as software diversity because it is the software that takes down
15 networks.

16 **Q. Several kinds of diversity have been mentioned in testimony. Will you more**
17 **completely explain “Software Diversity” and how that affected this incident?**

18 A. As I have explained in prior testimony, software underlies all modern
19 telecommunications devices. Error (“bug”) free software, especially in large complex
20 devices, does not exist. Errors are a fact of life. While software developers have many
21 tools available to them to detect the presence of errors in their code, they are not

¹² Rosen, Exh. BR-16C (Comtech Confidential Response to Public Counsel Data Request No. 3).

1 foolproof. Software failures are almost universally the underlying problem that causes
2 an entire 9-1-1 system to fail. The triggering event might be a human, hardware, or
3 environmental failure, but the underlying reason the entire system fails is software.

4 The fundamental reason this is true is that our most common defense against
5 total system failure is redundancy. A redundant system does not depend on a single
6 instance of anything: there are multiple instances, geographically dispersed, so that a
7 failure in one instance can be compensated for by another instance. We say that we
8 have no single point of failure in such a system because redundancy ensures a single
9 failure, or in many cases, multiple failures, will not bring the system down.

10 Unfortunately, the complex devices from which we build 9-1-1 systems, all run the
11 same software. The vendors of the systems select one vendor who writes the software
12 once, and all instances run the same software. This means the *software* is a single
13 point of failure and redundancy in such an example would not prevent total system
14 failure. A bug in the code is a bug in every instance of that device in a system.

15 The only defense against this problem is to use interoperable devices based on
16 standards. If devices conform to carefully constructed standards, devices from
17 multiple vendors can perform nearly identically to each other and interoperate with
18 each other. Not every function is likely to be standardized. For example, the
19 management and provisioning of the device may not conform to standards (indeed,
20 standard may not exist for those functions), but the function of the device *can* be
21 standardized in a way that multiple vendor's devices can be fielded in a single
22 system.

1 Major telecom service providers used to qualify two or more vendors, insist
2 the vendors conform to standards, and field more than one vendor's devices in a
3 network. If a software bug affected all of a vendors devices, it was highly unlikely to
4 affect another vendor's devices, and the entire network would not fail. However, cost
5 considerations have led those service providers to abandon multiple vendor networks.
6 Thus, it is now uncommon to see multiple vendors supplying the same function in
7 one network. That makes all such networks subject to the single point of failure: the
8 software. Customers do not have an option to choose a service provider who would
9 not be subject to that problem because they all use single vendors.

10 The Green network failed because a software failure was a single point of
11 failure in the network, and that caused the widespread outage to the 9-1-1 network.

12 **Q. Could software diversity have prevented this incident?**

13 A. Possibly. Despite CenturyLink's claim that version differences between its networks
14 offered some protection, a single vendor and a single version of that vendor's
15 software was installed on the network that failed. Moreover, the other network failed
16 earlier in the year. So, deploying different versions of software from a single vendor
17 did not prevent network failure.

18 In this specific case, if there were two vendors and the network were designed
19 reasonably, it is likely that there would have been at least one link that worked at any
20 time. CenturyLink had recent experience, the Red network failure, where a software
21 fault in Infinera networks could take down the entire network. In this incident, there
22 was a different fault than what caused the first incident, but it had the same result: the

1 entire network failed.

2 Indeed, CenturyLink's expert witness Turner clearly states that software
3 diversity is an essential safeguard:

4 Best network engineering practices require network redundancy for
5 critical network infrastructure such as signaling. Network redundancy
6 is implemented by means of ensuring route diversity. Route diversity
7 does not simply mean geographic diversity of the transport facilities for
8 the network. Its meaning is much broader. It requires that redundant
9 network components must travel on different routes not only using
10 diverse transport facilities, but also with no single points of failure either
11 from a physical equipment *or software standpoint*.¹³

12 Turner repeatedly cites the need for "no single points of failure", but the
13 software was a known single point of failure. CenturyLink had observed a software
14 single point of failure in the Red network failure. Software as a single point of failure
15 is a very well-known problem, and it has occurred several times, as I stated in the
16 Response of Public Counsel to CenturyLink's Data Request No. 17.¹⁴

17 **Q. How did all types of diversity affect this incident?**

18 A. All four links in the part of the network from TNS to Comtech were provisioned on
19 the same CenturyLink network. There was no network diversity. The incident caused
20 failures on all the switches in the network used by the interconnect, and it failed.

21 There was also no software diversity, but it did not affect other networks that
22 were running the same brand of switches in CenturyLink and there were version
23 differences in the networks.

24 We do not know if there was geographic diversity, but we do know Comtech

¹³ Turner, Exh. SET-1TC at 25:5-11 (emphasis added).

¹⁴ Rosen, Exh. BR-31 (Public Counsel's Response to CenturyLink's Data Request No. 17).

1 did not request it.

2 **Q. Refer to Exhibit MDV-1TC at 5–6. Valence claims you do not understand how**
3 **supplier diversity affects CenturyLink networks. Please respond.**

4 A. My statement was, “CenturyLink built its optical network using multiple optical
5 network switches supplied by one vendor, Infinera Corporation. Had CenturyLink
6 deployed two vendors, the nationwide failure that impacted Washington’s 9-1-1
7 system either would not have happened, or the scope and duration of the failure
8 would have been reduced dramatically.”¹⁵ That is a completely accurate statement, as
9 demonstrated by the discussion above regarding diversity. The failed “Green”
10 network was constructed with switches supplied by a single vendor, Infinera. Had
11 there been two vendors, the 9-1-1 failure would likely not have happened. While
12 Valence explains that CenturyLink has more than one network and therefore, it could
13 offer a form of supplier diversity, in my opinion that is not actual or functional
14 supplier diversity. Importantly, at least one of the networks that CenturyLink offered
15 as part of its definition of supplier diversity used the same manufacturer.

16 **Q. Refer to MDV-1TC at 11-20. Valence describes the differences between the**
17 **“Red” and “Green” network and states that these differences were significant**
18 **enough that CenturyLink had no reason to believe the Green network could fail**
19 **in the same way the Red network failed. What is your reaction to that?**

20 A. The Red network failure showed that it was possible for the entire optical network to
21 fail when the management channel, which was not being used, became clogged with

¹⁵ Direct Testimony of Brian Rosen, Exh. BR-1CTr at 20:5–9 (footnote omitted).

1 packets and exhausted resources in the switch to the point where revenue traffic was
2 impeded. When doing root cause analysis on highly available systems, the root cause
3 is not *what* failed. The root cause is *why that failure caused the entire system to fail*.

4 Highly available systems are supposed to be immune to failures that impact
5 the entire system. The failure to focus on the second half of the analysis is a very
6 common oversight in root cause analysis. The cause of the immediate failure is not
7 the root cause (or at least, not the root cause we care the most about). The more
8 relevant root cause is why the entire system failed even when the immediate failure
9 occurred.

10 Consider an analogy of a bridge that collapsed. Suppose that salt corroded a
11 strut, and the strut failed, triggering the collapse. The root cause is not that the strut
12 collapsed. The root cause is that corrosion caused by salt on a single strut took the
13 entire bridge down.

14 The root of the failure here was that the network management system could
15 create a packet storm that shut down the network. Infinera only focused on what
16 caused the packet storm. CenturyLink accepted this explanation and compounded it
17 by not insisting Infinera disable the management channel on the Green network. Bad
18 packets happen. Bugs in code handling packets happen. But, if the entire network can
19 be disabled because it is possible for the management channel to create a packet
20 storm, the management channel should be turned off until it is no longer possible for
21 a packet storm on the management channel to take down the network. As an example,
22 Infinera could have disabled the ability of the management channel to send any

1 packets. It could have also refused to process any received packets. That the cause of
2 the packet storm in the Red network was different from the cause of the packet storm
3 in the Green network is immaterial. The real problem was that the network could
4 generate a packet storm and be taken down by such a packet storm, regardless of
5 cause.

6 Further, packet storms may arise under various scenarios. CenturyLink's
7 networks should have been resilient enough to withstand packet storms, regardless of
8 cause.

9 **Q. Refer to Exhibit MDV-1TC at 10–11. Valence opines that the outage on the**
10 **green network was not foreseeable. Was it?**

11 A. As I have explained, the evidence shows that CenturyLink knew that packet storms
12 on the management channel were possible, resulting in the network going down.
13 CenturyLink knew that any Infinera-based network would be vulnerable to packet
14 storms. In my professional opinion, CenturyLink should have insisted that Infinera
15 disable the management channel and fix the root cause so that it was not possible to
16 take down the network if a packet storm occurred on the management channel. The
17 management channel should have been disabled in such a way that it could not send
18 packets, and reception of packets could not tie up the switches' resources.

19 **Q. Refer to Exhibit MDV-1TC at 20–22. Valence insists that CenturyLink offers**
20 **diversity options that are available by essentially checking a box and paying a**
21 **small fee. He cites the following text:**

22 **You can order diverse routing for 911/E911 circuits if facilities are**
23 **available. These trunks must be provisioned to conform to the**

1 **standard CAMA signaling format. When CenturyLink facilities are**
2 **available, CenturyLink will comply with diversity of facilities and**
3 **systems as ordered by you. Where there is alternate routing of**
4 **911/E911 calls to a PSAP in the event of failures, CenturyLink shall**
5 **make that alternate routing available to you.¹⁶**

6 **What is your response?**

7 A. Beyond the statement cited by Valence, I do not know what CenturyLink advises
8 customers about diversity. Regardless, that specific statement by Valence is a red
9 herring because it is not applicable to what Comtech ordered. It ordered facilities that
10 used SS7 signaling, not CAMA, which is the only option the quoted statement
11 describes.

12 **Q. Refer to Exhibit MDV-1TC at 9–10; Exhibit SET-1TC at 9:26–29; and Exhibit**
13 **CDK-1TC at 13:4–7. CenturyLink’s witnesses claim that the reason for the**
14 **failure was that Comtech did not use supplier diversity in connections between**
15 **TNS and its system. Is that true?**

16 A. Yes. If Comtech had provisioned the SS7 signaling links with supplier diversity (in
17 this context, network diversity), the failure would not have happened. But, if
18 CenturyLink had agreed to the IP interconnect Comtech proposed, the failure would
19 also not have happened. If CenturyLink had used software diversity in its Green
20 network, the failure would not have happened. If CenturyLink/Infinera had disabled
21 the management channel, the failure would not have happened. If CenturyLink had
22 used its own STPs (especially in-state STPS) rather than using TNS, the failure would
23 not have happened.

¹⁶ Valence, Exh. MDV-1TC at 21:2–7 (citing webpage: <https://www.centurylink.com/wholesale/pcat/911.html>).

1 Many errors were made here, **any one of which**, if undone or corrected,
2 would have avoided the failure.

IV. **TRANSITION RESPONSIBILITIES**

3 **Q. Refer to Exhibit CDK-1TC at 6–9; Exhibit SET-1TC at 40:8–10; and Stacy**
4 **Hartman’s Exhibit SJH-12C. CenturyLink’s witnesses claim the point of**
5 **demarcation was in the middle of the TNS network. Please explain what a point**
6 **of demarcation is.**

7 A. When a service provider provides a telecom service to a customer, or where two
8 service providers interconnect, it is routine to describe a “point of demarcation” that
9 defines when responsibility shifts from the customer to the service provider (and vice
10 versa) or where responsibility shifts from one service provider to another. In my
11 experience, the point of demarcation is typically described in the contract between the
12 parties, but may also be described in agreements between the parties beyond
13 contracts. One party cannot unilaterally assert the point of demarcation: it is an
14 agreement. The point of demarcation is important because if a failure occurs, the
15 contract usually specifies **who** is liable for failure (and what penalties may be
16 incurred) using the point of demarcation as the point at which liability shifts.

17 **Q. Based on your review, where was the point of demarcation at the time of the**
18 **outage?**

19 A. In Exhibit SET-7C, Comtech supplied a drawing of an IP-based interconnect, which
20 *proposes* a point of demarcation. Turner cites this as evidence of where the point of

1 demarcation should be.¹⁷ However, the interconnect shown in Exhibit SET-7C is not
2 the interconnect that was actually implemented because Comtech clarified that
3 CenturyLink rejected that proposal.¹⁸ As a result, the point of demarcation identified
4 by Turner was not the point of demarcation between CenturyLink and Comtech at the
5 time of the December 2018 outage.

6 Further, Turner places the point of demarcation in the middle of the TNS
7 network,¹⁹ on which neither Comtech nor CenturyLink had any control, visibility, or
8 influence. In my professional experience, that is not a tenable point of demarcation.
9 Comtech provided a drawing showing where it believed the point of demarcation was
10 at the time of the outage: at Comtech's first piece of equipment.²⁰ That point is at
11 least a reasonable and viable point of demarcation.

12 Even though Comtech identified a viable point of demarcation, there was no
13 agreement between CenturyLink and Comtech regarding where the point of
14 demarcation actually existed. As the underlying contracts and amendments make
15 clear, the point of demarcation was simply not specified between CenturyLink and
16 Comtech. This is highly unusual, as the point of demarcation is usually carefully
17 defined in contract. Without an agreed point of demarcation, it is nearly impossible to
18 assign responsibility at any specific point in the network. That there is no point of
19 demarcation means CenturyLink **cannot** establish that it was not responsible for a

¹⁷ Turner, Exh. SET-1TC at 43.

¹⁸ Rosen, Exh. BR-32C (Comtech's Response to Public Counsel Data Request No. 31).

¹⁹ Rosen, Exh. BR-5 (CenturyLink Supplemental Response to Public Counsel Data Request No. 7, Attachment PC-7a).

²⁰ Rosen, Exh. BR-32C (Comtech's Response to Public Counsel Data Request No. 31, Attachment).

1 failure in the middle of the 9-1-1 network, especially since the actual part that failed
2 was a **CenturyLink optical network** that carried part of the 9-1-1 network.

3 **Q. Why is CenturyLink's assertion that the point of demarcation was in the middle**
4 **of TNS network untenable?**

5 A. Based upon my professional experience and review of the evidence, it appears to me
6 that CenturyLink defined how the interconnect would work and instructed Comtech
7 to use TNS as the SS7 signaling network. Comtech obliged. With TNS in the middle,
8 there is no obvious point of demarcation between CenturyLink and Comtech.
9 CenturyLink now claims the point of demarcation is literally in the middle of the TNS
10 network. Yet, that point is beyond where Intrado connects to TNS and before
11 CenturyLink connects to TNS. This is untenable, because TNS did not identify the
12 location of the point of demarcation within its network. Furthermore, a point in the
13 middle of TNS's network would not have been observable or manageable by either
14 CenturyLink or Comtech.

15 **Q. Do you believe Comtech's asserted location for the point of demarcation is**
16 **reasonable?**

17 A. Comtech claims the point of demarcation is in the handoff between TNS and
18 Comtech.²¹ Further, it claims that the point of demarcation is on its side of the
19 handoff. This is a reasonable point of demarcation because two of the links that failed
20 were ordered by TNS; two were ordered by Comtech.²² That makes it harder to assert

²¹ Rosen, Exh. BR-32C (Comtech's Response to Public Counsel Data Request No. 31, Attachment).

²² Rosen, Exh. BR-15C (Comtech Confidential Response to Public Counsel Data Request No. 1, with Confidential Attachment A).

1 that the TNS side of the handoff was the point of demarcation. Since CenturyLink
2 provided the links and it was a CenturyLink network that failed, it lends credence to
3 the argument that the point of demarcation was on the Comtech side of the TNS-to-
4 Comtech links.

5 I am not a lawyer, but I have extensive experience in this industry including
6 reviewing and advising relating to contracts denoting a point of demarcation. In my
7 opinion, the fact that there is not an agreed upon point of demarcation means that
8 CenturyLink cannot claim the outage is all Comtech's responsibility.

9 **Q. Refer to Exhibit SET-1TC at 40–43. Turner asserts that CenturyLink's**
10 **responsibility for the network under the contract transitioned to Comtech when**
11 **Comtech became the Covered 9-1-1 Service Provider. Do you agree?**

12 A. No. In the contract between Washington Military Department (WMD) and
13 CenturyLink, there is a list of services CenturyLink is required to provide. One of the
14 services listed is "network".²³ In this industry, "network" is generally understood to
15 be the signaling and voice path, plus the interconnects for auxiliary services such as
16 location. We distinguish the network from the *services* that ride on the network.

17 If the entire system had been provided by CenturyLink, the links that failed
18 would clearly be part of "network". There was another service, "Covered 9-1-1
19 Service Provider," which is a term used by the FCC to define the service provider

²³ Rosen, Exh. BR-4C at 15 (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196 at 14).

1 who delivers calls to a PSAP. The term is defined by the FCC rules.²⁴ The contract
2 made CenturyLink responsible for, among other things “network” and “Covered 9-1-
3 1 Service Provider”. Contract modifications were made to accommodate the
4 transition from CenturyLink to Comtech. Amendment M specifically discussed the
5 transition and clearly stated that when a PSAP transitioned from the CenturyLink
6 ESInet to the Comtech ESInet, then Comtech became the Covered 9-1-1 Service
7 Provider.

8 While the responsibilities of a Covered 9-1-1 Service Provider could have
9 been expanded by contract, and some aspects of network are most often assumed by
10 the Covered 9-1-1 Service Provider, the contract expressly mentions “network” (and
11 “transport”) independently of “Covered 9-1-1 Service Provider”.²⁵ Based upon the
12 plain language of the contract, clearly, WMD believed it was important that
13 CenturyLink be responsible for network and transport in addition to being the
14 Covered 9-1-1 Service Provider. Amendment M did not relieve CenturyLink of the
15 responsibility for “network” or “transport”. Nor did any other amendment.

16 That means that CenturyLink was still responsible for the network and
17 transport at the time of the outage. Indeed, WMD has stated it “believes CenturyLink
18 retained a role, and thus an obligation under the Washington Military (WMD)
19 CenturyLink, Contract No. E09-106, until there were no parts of the originating

²⁴ At the time Amendment M to the WMD and CenturyLink contract was executed, the FCC definition of “Covered 9-1-1 Service Provider” was found at 47 C.F.R. §12.4(a)(4). Today the definition is found at 47 C.F.R. §9.19(a)(4). The definitions are the same.

²⁵ Rosen, Exh. BR-4C (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196).

1 network nor the terminating network connected to the CenturyLink/Intrado ESInet.”²⁶

2 If I were advising WMD, I would not relieve either CenturyLink or Comtech
3 from responsibility for both the network and transport because of the complexity of
4 having an SS7 network in the middle of two IP networks. Indeed, the lack of a clear
5 point of demarcation is indicative of the issues that can arise in transitions. Both
6 CenturyLink and Comtech should have been checking each other, verifying that the
7 entire network was designed and built to meet both companies’ 99.999 percent
8 availability requirement. Both should have been intimately involved in the design and
9 provisioning of the entire interconnect. CenturyLink was responsible for “network”
10 and “transport,” and they were responsible for the entire network, and all of the
11 circuits, including the part that failed in December 2018.

12 **Q. Refer to Valerie Lobdell’s Exhibit VL-1TC at 4:8–9. Lobdell describes the three**
13 **phased transition approach required by WMD to be “unnecessarily complicated**
14 **and introduced unknown risks.” Do you agree?**

15 A. No. The phased transition approach was necessary. There are three parts in 9-1-1
16 networks: the ingress, the core, and the egress. The ingress is the connections from
17 the Originating Service Providers (OSPs) to the 9-1-1 network. The egress is the
18 connections from the 9-1-1 network to the PSAPs. It is not feasible to have a “flash”
19 cutover from one network to the other due to the high risk involved with changing too
20 many things at the same time. Instead, OSPs and PSAPs must be migrated one at a
21 time. While that migration is in process, calls from any OSP to any PSAP must work.

²⁶ Rosen, Exh. BR-27 at 3 (WMD Supplemental Response to Public Counsel Data Request No. 7).

1 **Q. Please describe how such transitions ordinarily take place.**

2 A. When performing a migration like this, both the existing and new vendors must have
3 interconnections between their systems. For example, a call from an OSP that had
4 transitioned to the new network must be able to be placed from an OSP that had not
5 yet transitioned. It is very common that all the transitions on one side are completed
6 before any on the other side are completed so that all PSAPs may be transitioned to
7 the new vendor while all OSPs remain untransitioned, or vice versa. Further, it is
8 essential that calls originally sent to a transitioned PSAP be able to be transferred to
9 an untransitioned PSAP, regardless of whether the OSP was transitioned or
10 untransitioned.

11 Even if OSP and PSAP transitions can be interleaved, because any OSP must
12 be able to send a call to any PSAP, an interconnection between the two networks is
13 required. Further, both networks must make routing decisions. Regardless of order,
14 one network may start routing only to discover that the destination is on the other side
15 of the interconnect, and when the other side gets the call, they must route it to the
16 right PSAP. That is exactly how this migration was specified. Because a flash cutover
17 is not feasible, both networks must be interconnected, and both must route.

18 In this case, the choice to use an SS7 interconnect between the two IP
19 networks increased the complexity and risk, not the choice to use a phased transition.
20 It would have been *much* simpler to connect the two IP networks and route calls from
21 one to the other via the IP based signaling that both used. Furthermore, calls must be
22 able to be transferred from one PSAP to another. When a call transfers from an

1 untransitioned PSAP to a transitioned PSAP, or a transitioned PSAP to an
2 untransitioned PSAP, it must occur on some interconnect between the systems.

3 I will note that interconnection of ESInets, rerouting of calls between them,
4 and transfer of calls between them were not standardized at the time of this event.
5 However, standards, developed by NENA now exist,²⁷ and they describe a design
6 very similar to what Comtech originally proposed. This underscores the fact that
7 many experts agree with the basic approach Comtech proposed and CenturyLink
8 rejected.

9 **Q. Refer to Exhibit CDK-1TC at 6:17–18. Klein states that CenturyLink’s**
10 **suggested way to accomplish the transition was a recommendation “that calls**
11 **destined for a Comtech PSAP be flash-cut to Comtech with CenturyLink out of**
12 **the call flow altogether.” What is your opinion of that proposal?**

13 A. I am very surprised that such a suggestion was made. Unless one OSP only serves one
14 PSAP, then calls from one OSP must be able to go to both untransitioned
15 (CenturyLink PSAPs) and transitioned PSAPs (Comtech PSAPs). If the OSP is
16 untransitioned, then it would have to go through the CenturyLink network, some of
17 its calls would have to interconnect to the Comtech network and be routed to the
18 transitioned PSAP. Calls to the untransitioned PSAP from that OSP would remain on
19 the CenturyLink network. If the OSP transitioned, then some of its calls would have
20 to be sent to the CenturyLink network for delivery to the untransitioned PSAP. If all

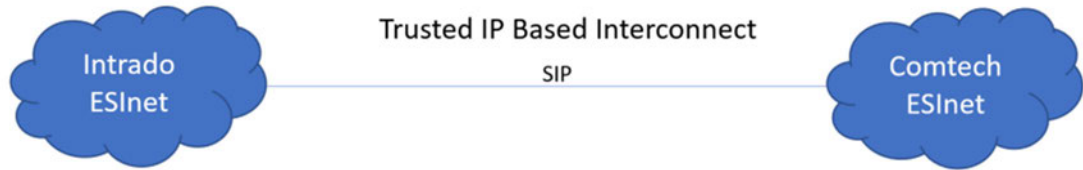
²⁷ Nat’l Emergency Number Ass’n (NENA), *NENA i3 Standard for Next Generation 9-1-1* (2021),
https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-010.3b-2021_i3_stan.pdf.

1 OSPs were transitioned before any PSAP was transitioned, then when a PSAP
2 transitioned, CenturyLink would not be in the path, but before then, unless they flash
3 cut *all* the OSPs to Comtech at once, there would be exactly the arrangement that was
4 used, but Comtech would have to route calls to CenturyLink and CenturyLink would
5 route calls to untransitioned PSAPs.

6 WMD chose to transition PSAPs before OSPs, but transitioning OSPs before
7 PSAPs still requires the kind of arrangements that were used. When all the PSAPs
8 were transitioned, the final phase transitioned the OSPs, one at a time. That would
9 effectively be “flash cut” of an OSP from CenturyLink to Comtech, but it is only
10 possible because all the PSAPs were transitioned first. I am not aware of any
11 compelling reason to transition OSPs before PSAPs, but I am certain that doing them
12 one at a time is much preferred over doing them all at the same time. If the PSAPs are
13 transitioned one at a time, then calls will transition both networks for some calls until
14 all OSPs and all PSAPs are cut over.

15 **Q. Refer to Exhibit CDK-ITC at 6 and 10. Klein provides diagrams more closely**
16 **illustrating the call path at the time of transition. Do you have any comment on**
17 **those diagrams?**

18 A. Yes. Figure 2 “Non Simplified Phase 1 call flow” illustrates the clear danger of
19 interconnecting two IP networks with an SS7 network. If the IP networks were
20 interconnected in the simplest way, where CenturyLink and Comtech trusted each
21 other (which, for this transition, I think they should have) then the diagram would
22 look like this:

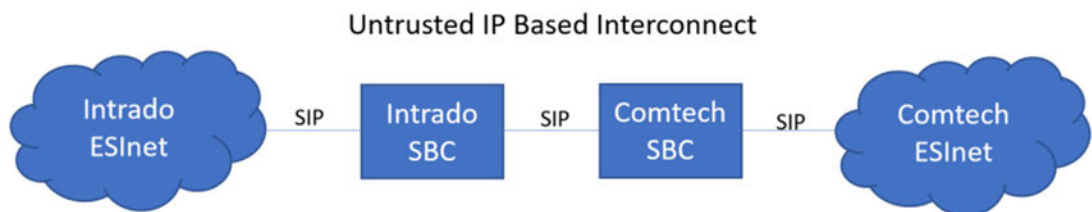


1

2

If they did not trust each other, then the diagram would look like this:

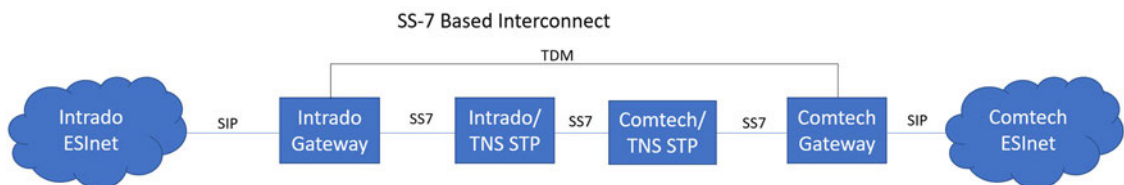
3



4

5

Instead what they implemented is this:



6

7

Q. Refer to Exhibit SET-1TC at 41–43. Turner claims that “Covered 9-1-1 Service Provider” is much broader than the definition used by the Code of Federal Regulations and uses another FCC document to attempt to show that it is more comprehensive. Turner then disputes that the lack of relief from the responsibility for “network” makes CenturyLink liable for the failure. Would you like to comment?

8

9

10

11

12

13

A. In this situation, the contract specifically called out “network” independently of “Covered 9-1-1 Service Provider”. In a fully transitioned network, we would expect

14

1 the Covered 9-1-1 Service Provider to “aggregate 911 traffic from an originating
2 service provider and deliver it to a 911 call center”,²⁸ but that would not be the case
3 here. CenturyLink was aggregating 9-1-1 traffic from an originating service provider
4 and was part of the delivery path to the 9-1-1 call center. “Network” and “Transport”
5 means the underlying communications system rather than the services that rides on it,
6 so making CenturyLink (and, jointly Comtech) responsible for them does not
7 interfere with Comtech being the Covered 9-1-1 Service Provider.

8 **Q. Refer to Exhibit SET-1TC at 44:6–13. Turner objects to your testimony that the**
9 **ALI connections between CenturyLink and Comtech were provisioned over IP**
10 **and did not fail. Turner claims they were provided by NoaNet. Is that true?**

11 A. No. NoaNet was used by Comtech to get IP connections to PSAPs.²⁹ I believe the IP
12 connections for ALI between Comtech and CenturyLink [REDACTED]

13 [REDACTED]

14 [REDACTED].³⁰

V. FAILURES IN THE GREEN NETWORK

15 **Q. Refer to UTC Staff witness James Webber’s Exhibit JDW-1CT at 24:6–16 and**
16 **Exhibit SET-1TC at 52–55. Webber suggested that the management channel**

²⁸ F.C.C., *911 Reliability* (last updated Dec. 20, 2021), <https://www.fcc.gov/911-reliability>. At the time Amendment M to the WMD and CenturyLink contract was executed, the FCC definition of “Covered 9-1-1 Service Provider” was found at 47 C.F.R. §12.4(a)(4). Today the definition is found at 47 C.F.R. §9.19(a)(4). The definitions are the same.

²⁹ Rosen, Exh. BR-29C (Comtech Response to Public Counsel Data Request No. 9).

³⁰ Rosen, Exh. BR-4C at 31 (WMD Response to Public Counsel Data Request No. 3, Attachment Washington State Military Department Contract E09-196 Amendment M Scope of Work).

1 **should have been disabled. Turner provides several statements that claim**

2 **CenturyLink did the right thing. Do you agree?**

3 A. No. First, Turner suggests that the management channel (Infinera General
4 Communications Channel or IGCC) was disabled.³¹ It was not. It was indirectly
5 prohibited from operating due to the software limiting packets to a certain size, which
6 only filtered packets that were exactly the size expected to be found on the
7 management channel, or smaller. That is not disabling the channel. If the channel
8 were disabled, there should be no resources consumed by sending or receiving
9 packets. CenturyLink claims the Red management channel was essentially “disabled”
10 and yet a packet storm took it down. Clearly, this was not an effective disablement.
11 Specifically, this supposedly disabled management channel was capable of *sending*
12 packets.

13 Then Turner deflects blame from CenturyLink and places it on Infinera. While
14 customers like CenturyLink do follow the advice of the supplier, they do not do it
15 blindly. Having been employed in my past by large provider of equipment carriers
16 like CenturyLink, I know, as Turner surely knows, that large service providers do not
17 take such advice at face value, but rather ask lots of questions, and very often instruct
18 their vendor to be more conservative than the vendor suggests. This is the nature of
19 large service providers: they are inherently risk averse. Having experienced the Red
20 network failure, CenturyLink should have instructed Infinera to make sure that under
21 no circumstances could a packet storm be created on the Green network. That would

³¹ Turner, Exh. SET-1TC at 55.

1 mean something more aggressive than just using a packet length filter.

VI. CONCLUSIONS

2 **Q. Does this conclude your cross-answering testimony?**

3 **A. Yes.**