The following responses are provided jointly on behalf of AT&T, CenturyLink, Charter Communications and Cox Communications.

Information Technology Advisory Board – Study of Peering

1. **Does the doctrine of federal preemption effectively prevent a state from enforcing any statutory or regulatory provisions affecting "arrangements for Internet traffic exchange" include peering?**

In its 2015 *Order*, the Federal Communications Commission ("FCC") found "arrangements for Internet traffic exchange," including peering, are broadband internet access service subject to the FCC's authority under Title II of the Communications Act ("Act").[1] The FCC retained targeted authority over such arrangements through section 201, 202, and 208 of the Act, but forbore from a majority of other provisions in the Act.[2]

Nevada cannot enforce a statutory or regulatory provision affecting "arrangements for Internet traffic exchange." The FCC classified broadband Internet access service as jurisdictionally interstate for regulatory purposes.[3] Further, the FCC specifically noted that states may not continue to apply or enforce any provision from which the FCC granted forbearance.[4] The FCC also announced its "firm intention to exercise preemption authority to preclude states from imposing obligations on broadband service that are inconsistent with the carefully tailored regulatory scheme" adopted by the FCC.[5] Any attempt by Nevada to impose an in-state peering obligation would be inconsistent with the regulatory scheme established by the FCC.

[1] Protecting and Promoting the Internet, Report and Order on Remand, Declaratory Rulings and Order, GN Docket No. 14-28, FCC 15-24 (rel. March 12, 2015)("*Order*"), *affirmed on appeal*, U.S. Telecom Ass'n v. FCC. No. 15-1063, slip op. at 97-106 (D.C. Cir. June 14, 2016), *pets. for en banc rehearing pending*; para. 195 ("[t]he definition of broadband Internet access service includes the exchange of Internet traffic by an edge provider or intermediary with the broadband provider's network."); para. 202 ("…arrangements for Internet traffic exchange (which are subsumed within Broadband Internet access service…")' para 204 ("As a telecommunications service, broadband Internet access service implicitly includes an assertion that the broadband provider will make just and reasonable efforts to transmit and deliver its customers' traffic to and from 'all or substantially all Internet endpoints' under sections 201 and 202 of the Act.") See also, para. 204 ("…disputes involving a provider of broadband Internet access service regarding Internet traffic exchange arrangements that interfere with the delivery of broadband Internet access service end user's traffic are subject to our authority under Title II of the Act.")

[2] Order, para. 195

[3] *Order*, para. 431

[4] Order, para. 432.

[5] Order, para. 433.

2. **If the physical world threat over public internet facilities between two points in Nevada is not realistically affected by an in-state peering requirement, should Nevada instead legislate minimum physical security requirements for data centers in Nevada where peering of public internet traffic takes place as the most effective way to reduce risk in the physical world?**

An in-state peering requirement will not reduce the exposure of cyber threats against Nevada state entities. Any Nevada state service, data, or critical infrastructure exposed to the public internet is vulnerable to a variety of cyber-attacks, including Distributed Denial of Service ("DDOS") attacks and the infiltration/exfiltration of data. In order to protect such critical infrastructure and/or data from the public internet, the industry best practice is for the data to be: 1) encrypted at the end points; 2) within a private virtual private network ("VPN") context (not routed on the public internet); or 3) transported over a dedicated private line between end points.

Specifying additional physical security requirements for data centers where peering traffic takes place would not be any more effective on potential data compromises. Since most data centers contain the same critical business system data that would potentially be transported over the internet, a holistic approach to physical security would be required. It would not make sense to add additional physical security around peering if the physical servers where the data resides does not have the same set of physical security standards applied. Requiring in-state peering is like requiring only one door to be locked of a multi-door building.

3. **What percent of successful data compromises have been directed at data in transit as compared with those directed at data at rest? In Nevada as compared with the United States as a whole? How will an in-state peering requirement increase the security of in-transit data originating from, or destined for, a location in Nevada?**

The responding companies are not aware of any specific information separating data compromises in transit compared to those at rest, let alone in Nevada compared to the United States as a whole. An in-state peering requirement does not increase the security of data being transmitted in/out the State of Nevada due to reasons cited in question #2.

4. **Will an in-state peering requirement result in an increase in service quality that is perceptible to the end user? How do you know?**

An in-state peering requirement would not perceptibly increase service quality to end users in Nevada as there are too many variables external to peering that impact service quality. In-state peering would also be a significant departure to the proven long-standing industry practice of how networks interconnect to exchange internet traffic. National and global networks typically interconnect in a few regions that encompass large geographies that include multiple states.

Adding peering within the state of Nevada is likely to result in companies having to re-architect how networks are configured, adding inefficiencies and unnecessary cost, because every additional peering exchange is another "entry point" into the network that must be managed. The more entry points, the more difficult it is to manage network traffic. Additionally, each one

of these "entry points" becomes another security threat to the network. In order to protect the end user experience and in some cases, sensitive information, companies prefer to maintain a reasonable number of entry points into the network. Each additional entry point becomes another target for security attacks, making the network more vulnerable.

5. **What would be the effect on Nevada end users if contiguous states enacted in-state peering requirements identical to those enacted in Nevada? If all states enacted identical requirements? If all countries enacted similar provisions?**

If multiple states or all states, or even all countries, required local peering arrangements, most customers would see few, if any, positive impacts to the user experience. Adding more and more peering points to a network with an already richly established fabric provides diminishing returns.

Networks benefit when interconnecting at large scale. Peering works precisely because ISPs, CDNs (Content Delivery Networks), and content providers all work together so that major network entities meet at as many exchange points as efficiently needs and the market otherwise dictate. For this reason, best practices within the internet community long ago have generally resulted in the selection of a few carefully chosen geographic sites throughout the country as interconnect points. This practice has been in place for well over 20 years. The Internet has flourished as a result.

This leads to the last point - cost. Adding additional peering points in some/all states, with associated colocation, circuit, fiber and construction costs, would be prohibitive, with no demonstrable end user benefit.

6. **To carriers (secondarily to governments): Do you provide facilities and/or services considered essential to the continued, non-degraded, functioning of government private networks? Are these facilities and/or services currently subject to competition, that is, could a competitor replace the facilities and/or services you provide?**

Numerous providers offer services to multiple residential/commercial and government locations. These services allow for both commercial and government entities to conduct business with the outside world, and connect peer to peer with other locations internally.

7. **Discuss the public policy considerations that would support the financial risk of in-state peering being borne by one set of entities while the proposed benefits of in-state peering would be conferred on another set of entities.**

As outlined in the response to Question 4, there will be no material benefit conferred by a mandatory in-state peering requirement and it will impose significant costs on providers. The end result is that such a requirement would constitute a tax on ISPs, an exaction by the state that provides no direct benefit to the providers (or any other entity).

8. **What agency would determine whether the in-state peering requirements were met for the purpose of state procurement actions? For the purpose of local government procurement actions? How would its decisions be enforced? What attendant statutory or regulatory changes would be required? For example, could an entity object to a contract award on the basis of non-compliance with an in-state peering requirement even though that entity did not participate in the relevant procurement process (an RFP or sole source procurement justified by a lack of vendors capable of supplying needed communications facilities and/or services)? Are the costs of the oversight and enforcement efforts justified by the likely benefits of an in-state peering requirement?**

It is not clear whether any existing state agency has the expertise or capacity to monitor a mandatory in-state peering requirement and ensure that every state and local procurement process complied with the obligation. It would require the continuous updating of a database of the companies required to comply with the mandate as well as monitoring all state and local procurement procedures to ensure that entities responding to RFPs were compliant with the mandate.

Significant changes in state and local procurement laws would most likely be required to give the state agency or agencies veto authority over the awarding of a contract to a non-compliant entity, or the ability to challenge and rescind an award after it is made. Disqualified entities would likely challenge decisions based on inaccurate compliance data. As noted in the response to Question 4, the lack of benefits to any party, including end users, of a mandatory in-state peering requirement, more than outweighs the costs of creating a new oversight and enforcement process.

9. **What benefits, attributable to an in-state peering requirement, would appeal to an enterprise considering relocating to Nevada? Conversely, what enterprises, if any, would consider an in-state peering requirement as a negative factor in determining whether to relocate to Nevada?**

There is nothing appealing about requiring a service provider to expend capital to comply with an in-state mandatory peering requirement that brings no benefits to the provider or its customers (see response to Question 4). Such a requirement would be a disincentive to companies looking to relocate to Nevada.

10. **If the benefits of in-state transit are sufficiently great (see Questions 3 and 4), won't providers of services delivered over public internet facilities negotiate the use of wholly in-state fiber facilities in order to provide the best possible service to Nevada end users as a matter of self interest, thereby rendering an in-state peering requirement irrelevant? Software-defined networking (SDN) and SD-WAN technology purportedly allows network administrators to decouple network control from the underlying physical infrastructure.**

Peering discussions rarely include fiber as a topic since fiber is considered part of the base network infrastructure, and because fiber requirements are different for each company. Additionally, national network operators generally do not build business or network models that consider Internet connectivity for one individual stand-alone state; rather, network planners include multiple or groups of states in their models as part of their overall regional and national networking strategy.

In-state peering only is not an approach that large network operators generally consider in developing a peering strategy for a region or nationally. As a concept, in-state peering would only satisfy users that are locally embedded, and, while it may theoretically offer a better experience, it would be limited to only those users that have that narrow requirement. The reality of the Internet is that all users have an expectation of global reachability, and therefore internet data is expected to be available from almost every origin and destination point worldwide. This means that, both as a matter of connectivity and competition, network operators must consistently develop network deployment strategies that are national and global in scale in order to fulfill this real-world expectation of Internet users. As such, limiting peering to in-state only has little or no utility to the user/customer.

11. Are there emerging or anticipated technologies that would replace, in whole or in part, traditional routing functions and peering arrangements, thereby rendering an in-state peering requirement obsolete? If so, in what time frame are these technologies likely to emerge as significant substitutes for existing technologies and commercial peering agreements?

There are no anticipated technologies that would completely do away with peering relationships between networks. Some technologies and business arrangements may optimize routing over a peering infrastructure (e.g. SDN-WAN applications), and possibly require more extensive peering relationships, but traffic exchange between networks will ultimately continue to be arranged by some means of interconnection. The basis for these interconnections will vary greatly based on the type of companies exchanging traffic, what type/mix of internet traffic is being exchanged, and network infrastructure considerations.

12. What other issues, not covered by the foregoing questions, do you believe are relevant to the Peering Study undertaken by the Information Advisory Board (ITAB)?

Taken as a whole, the questions in the RFI are both thoughtful and comprehensive, and allow respondents to thoroughly address the necessary and relevant issues pertaining to the idea of in-state peering that should be considered in the present regulatory and technological environment.