Table of Contents

COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation into the Collocation Security Policies of Verizon New England Inc. d/b/a Verizon Massachusetts	)	D.T.E. 02-8

INITIAL BRIEF OF
ALLEGIANCE TELECOM OF MASSACHUSETTS, INC.

INTRODUCTION

In its January 24, 2002 Vote and Order to Open Investigation ("*Order*") at 1, the Department described this proceeding as follows:

> The purpose of this investigation is to review our prior findings with respect to access by personnel of other carriers to Verizon's central offices and other facilities, and to assess the security measures in place to protect those facilities. The Department intends to determine, through the presentation of evidence, which policies, if any, should be strengthened to safeguard telecommunications networks from tampering and thereby to ensure reliable telecommunications service to the citizens of Massachusetts.

This purpose is a worthy one. Telecommunications services are sufficiently important to the welfare of the state that they demand close scrutiny. This proceeding should have provided, and may still provide, an appropriate vehicle for such scrutiny.

So far, sadly, it has not. This is due to no fault of the Department. Rather, it is due entirely to Verizon's overarching desire to use this proceeding to drive its competitors out of its central offices and, thereby, out of Massachusetts. Verizon makes no attempt to hide this desire. On the third page of its panel testimony (Exh. VZ-MA-1), the Verizon witnesses state flatly: "Verizon MA believes that the most effective means of ensuring network safety and reliability is

to eliminate physical colocation entirely in all its COs, converting existing physical colocation arrangements to virtual and requiring that all future collocation arrangements be virtual only." This statement sets Verizon's tone in this proceeding. Verizon focuses only on the presence of CLEC personnel in its central offices ("COs"), utterly ignoring the Department's well-placed interest in assessing "the security measures in place to protect [Verizon's central offices and other facilities]." *Order* at 1. Verizon's approach has resulted in a record remarkable for its cynicism, in which Verizon itself argues that its security measures are inadequate, and can be improved only by implementing a series of measures that will exclude CLEC personnel from central offices.

There is simply no evidence in the record to support Verizon's extreme proposals. There is no evidence that CLEC personnel pose any threat to the telecommunications network, much less an unreasonable threat that could be mitigated only by excluding such personnel from Verizon facilities. On the contrary, the record shows that CLECs take their responsibility to the network every bit as seriously as does Verizon, as one would expect from companies that depend on the network to complete customer calls and thereby conduct their business. This absence of evidence is a direct result of Verizon's strategy, which was to present no evidence whatsoever regarding any facility in Massachusetts, relying instead on the tautology that "foot traffic" is a threat to the network, and CLEC personnel cause foot traffic; therefore, the presence of CLEC personnel should be reduced or eliminated altogether. As discussed below, this argument disintegrates under the mildest scrutiny.

Based solely on the lack of evidence, the Department would be justified in rejecting all of Verizon's proposals for addressing an alleged problem (the very presence of CLEC personnel in Verizon central offices) that has been shown not to be a problem at all. In addition, however, the

two central Verizon proposals (which would outlaw CCOE arrangements in other than separate and secure space, and ban physical colocation entirely in certain "critical" COs) should be rejected because they violate the Telecommunications Act of 1996, and the Department and FCC orders implementing the Act. Indeed, Verizon has been a serial litigant of this issue before the Department and the FCC, and appeared to have lost rather definitively until the tragic events of September 11th presented an opportunity to characterize CLEC access as a potential security threat. Notably, no other State commission or the FCC has sought to revamp colocation security procedures as a result of September 11th. Allegiance encourages the Department to soundly rebuff Verizon's proposals to thwart competition in Massachusetts under the guise of protecting the network.

I. THE RECORD SHOWS THAT CLECS ARE NOT A THREAT TO CENTRAL OFFICE SECURITY.

Verizon asserts that the Department should take steps to permanently limit or, in some cases, eliminate the presence of CLECs in Verizon central offices. Verizon identifies two bases for this recommendation. One is the presence of CLEC "foot traffic" in COs, and the other is "Verizon's experience with security breaches in Massachusetts and elsewhere" (Exh. VZ-MA-1, at 2). Verizon's argument is that the mere presence of CLECs in COs is a threat to network security and, therefore, the Department should reduce that threat by reducing CLEC presence or "foot traffic" in COs.

This argument is simply unsupported by any evidence in the record. There is no evidence that colocation security at a single Verizon CO is inadequate. There is no evidence that the mere presence of CLECs in Verizon COs is a threat to network security, whether or not CLEC equipment is commingled with Verizon equipment. In fact, there is no evidence of a single

security breach, much less a network-affecting incident, caused by a CLEC in Massachusetts. Thus, the Department should reject the central premise of Verizon's proposals, that the mere presence of CLECs in COs poses an inherent risk to network security that the Department should take drastic steps to reduce.

What the evidence in this case does support is a finding by the Department that CLEC personnel pose no threat that is different in nature or greater in magnitude than the threat posed by Verizon personnel or Verizon vendors or contract personnel with access to COs, and that Massachusetts COs have been remarkably free of network-threatening incidents involving CLEC personnel. These findings would not remotely support the drastic and anti-competitive changes in colocation policy Verizon would like the Department to make.

A. There Is No Evidence That Colocation Security Is Inadequate In Any Central Office In Massachusetts. To The Contrary, Verizon Massachusetts Has Not Experienced A Single Network-Affecting Incident Caused By The Presence Of Colocated CLEC Equipment In Its Central Offices.

Verizon's approach in this case has been to try to prove that its own security practices are inadequate and that its central offices are being exposed to an unacceptably high risk of network-affecting incidents, whether in the form of accidents or sabotage. Verizon's witnesses stated that its "proposed security measures and enhancements are necessary *because of the present network architecture and configuration of equipment and facilities* in Verizon MA's COs and RTs" (Exh. VZ-MA-1, at 5 (emphasis added)). In fact, Verizon opposed CLEC efforts to obtain any such information in order to be able to investigate its claim that the "configuration of its equipment and facilities" has created an unacceptable security risk. The only evidence in the record regarding actual conditions or events at Massachusetts COs is there only as a result of CLECs' and the Attorney General's discovery efforts. *See, e.g.*, Exhs. AG-VZ-1-1, AL-VZ-2-1.

This is a bizarre approach. The Department opened this investigation "to assess the security measures in place to protect" Verizon COs and other facilities. *Order* at 1. Verizon claims that its proposal is necessary because of its network architecture and configuration, but then argues that producing information and documentation about that architecture and configuration is burdensome and irrelevant.[1] Verizon's panel testimony discusses certain types of security measures, such as card reader access systems ("CRAS"), surveillance cameras, and security guards, but even these are mentioned only in passing as Verizon rushes to its judgment: CLECs are a threat and their presence must be limited or banned. As a result, the Department is left with no factual basis whatsoever upon which it could conclude that the colocation security measures at any of the 169 Verizon central offices in which CLECs are colocated is inadequate, much less that they are inadequate at each and every one of these facilities.

Verizon could have offered such evidence, but it chose not to do so. Verizon's own security expert, in fact, testified that before making any recommendations for security changes at a facility, one should conduct a risk assessment. When asked at the hearing whether "risk assessments are an important part of a process that leads to the adoption of appropriate security measures for the facility that's being assessed," Mr. Lawrence Craft, a Manager in Verizon's Security Department who is responsible for Verizon East's Physical Security/Access Control function, answered, "Most definitely" (Tr. 24). Mr. Craft also testified that "a risk assessment typically is done on a by-location basis." Id. When asked whether "the security measures that are eventually adopted should have some relation to the risk that's been identified for the particular facility, Mr. Craft responded:

> First, a particular building, or any building, needs to have a certain baseline security. After that, the answer is yes. Depending upon the risk assessment will

[1] *See* Verizon's Reply to Motion to Compel (May 20, 2002), at 1-5; Exh. AL-VZ-1-1, at 2-3.

> determine the amount or the type of security deployment or equipment within that building.

Id.

In this case, Verizon ignored the standard operating procedure laid out by its own security expert. In making its recommendations to the Department, Verizon relied on no risk assessments whatsoever, even where those proposals would exclude CLECs completely from a CO deemed "critical." Mr. Craft testified that neither Verizon nor any contractor on its behalf undertook a risk assessment that specifically addresses the banning of CLECs from "critical" COs (Tr. 39-40). Mr. Craft testified further that Verizon has not done risk assessments at three COs that house E911 switches, although Verizon maintains that the presence of such equipment could justify the banning of CLECs from those COs. Tr. 158; Verizon Response to RR-AL-VZ-1. In fact, Verizon has completed, at most, one or two risk assessments at its facilities in Massachusetts, and it did not even rely on those in reaching its conclusion that the Department should drastically revise its policy toward physical colocation. Tr. 195, 198-99 (Craft, Mattera, Reney).

It is hard to explain the utter absence of any CO-specific evidence in Verizon's testimony in support of its proposals. One explanation is that an unbiased risk assessment of any of its facilities would not identify colocation as a security threat. There is convincing evidence in the record to support this explanation. This evidence takes two forms. First, in response to an information request issued by the Attorney General, Verizon produced incident reports from two of its departments. *See* Exhibit AG-VZ-1-1. One set of reports comes from Verizon's Collocation Care Center, or "CCC." The other comes from Verizon's security department. These reports reveal that Verizon has never experienced a network-affecting incident caused by CLEC personnel. In its panel testimony, Verizon concedes as much. Exh. VZ-MA-1, at 21.

Thus, Verizon's dire warnings about the threat CLECs pose to the network notwithstanding, there has not been a single minute of service interruption caused by a colocated CLEC in Massachusetts.

Second, in response to an Allegiance information request, Verizon produced "Deputy Building Coordinator Security Inspection Reports." *See* Exh. AL-VZ-2-1. These reports reflected inspections conducted by Verizon personnel at Massachusetts central offices in October 2001, shortly after the September 11 attacks.[2] *See* Exh. AL-VZ-2-1. Verizon asked its Deputy Building Coordinators to perform these security inspections and "forward any deficiencies (any area determined to be "poor" or the answer to any question is marked "no") to" Mr. Craft's department. The Deputy Building Coordinators were directed to "use the Inspection Report to notify us of any deficiencies (where applicable) especially in the areas of guard service, access control, CCTV system, perimeter security and adherence to wearing Verizon IDs." Id. The form itself included the question "is a security assessment by Corporate Security required to correct any security vulnerabilities that exist?" If any such security vulnerabilities or deficiencies had been identified, the Deputy Building Inspector would have made Mr. Craft's office aware by faxing the inspection report (Tr. 173).

These Inspection Reports do not identify any "security deficiencies" or "security vulnerabilities" caused by the presence of CLEC personnel in Verizon COs. The deficiencies that were forwarded to Mr. Craft's office for review and further action relate more to lapses in Verizon's own security practices, such as making sure visitors and non-employees use the sign-in/out log (the most frequent deficiency cited). Verizon reported these deficiencies resolved by

[2] Although Verizon apparently intended that all of its COs be inspected, Verizon produced only 152 inspection reports, some of which were for facilities in which no CLECs were colocated. There are 20 or more COs with colocated CLECs for which no inspection report was produced, including a large CO in Boston's Back Bay. Tr. 171.

the end of November 2001. *See* Verizon Response to RR-AL-VZ-3 (Motion for Confidential Treatment pending). The Inspection Reports do not identify ongoing security deficiencies caused by CLEC personnel.

Thus, the Department has two pieces of evidence by which to assess the threat posed by CLECs to specific COs in Massachusetts. One is that Verizon itself cannot identify a single incident in which a CLEC's actions resulted in a single minute of outage in Massachusetts. The other is that Verizon's own security inspections performed a month after September 11th revealed no deficiencies related to the presence of CLEC personnel in Verizon COs. This evidence supports, even compels, a finding that physical colocation does not pose a sufficient security threat that the Department should change its colocation policies in any way, much less in a way designed to limit or eliminate CLECs from Verizon COs. Verizon offered no CO-specific evidence that would allow any other conclusion.

B. Verizon's Hypothesis That The Presence Of CLEC Personnel In Verizon COs Poses A Threat To Network Security That Is Any Different, In Nature Or Magnitude, Than The Threat Presented By Verizon Employees, Vendors, And Visitors Is Just That: An Unproven Hypothesis.

Rather than rely on any CO-specific data whatsoever, Verizon bases its proposal on the assertion that "the presence of physical collocation" carries with it an "increased potential for network harm." Exh. VZ-MA-1, at 2. At the hearings, Verizon witnesses repeatedly identified reducing "foot traffic" as the primary goal of its proposed measures and that, since physical colocation creates foot traffic, the Department should restrict or eliminate physical colocation in order to enhance CO security. Tr. 62, 138, 146. The threat posed by "foot traffic", however, is completely unproven.

Though Verizon presents the assertion as though it were self-evident, there is no evidence to support the claim that the very presence of CLECs in COs and the "foot traffic" they bring increases the risk of damage to the network. One would expect that a point so critical to Verizon's proposals would be bolstered by expert testimony and statistical analyses. Not so here. Verizon's witnesses merely repeated the assertion whenever they were challenged on the justification for the anti-competitive measures they are proposing. *See, e.g.*, Tr. 63, 117, 140, 157, 164; Exhs. VZ-MA-1, at 41; VZ-MA-2, at 2.

The Department cannot make a finding equating "foot traffic" with a threat of network harm without any evidence to support it. Verizon offers none. The conclusion is not one that can be drawn from mere intuition or unsupported "logic" as Mr. Craft suggests. Tr. 41. There are examples of intuition or logic leading to just the opposite conclusion. For example, if foot traffic alone increased the threat of harm, one would expect pedestrians to feel safer on an isolated street at night than they would on a busy sidewalk during morning rush hour. There may be a similar effect here. It may be that CLECs are "self-policing," as Verizon seems to view its own employees, so that the presence of CLEC employees in a CO decreases or at least does not increase the potential for network-threatening accidents or sabotage.

The evidence in the record supports just this conclusion. Verizon's panel testified that the number of colocations in Massachusetts increased from around 1992 through mid- to late-2000, followed by a decrease due to terminations by CLECs. (Tr. 732-33). Before the recent downturn, CLEC "foot traffic" in Verizon COs increased with the number of colocations. (Tr. 733-34). This situation creates a natural experiment to test Verizon's hypothesis that the threat of network harm increases in direct proportion to the presence of CLECs and the "foot traffic"

they bring.[3] The evidence in the record tends to disprove this hypothesis. The number of a network-affecting incidents involving CLECs in Massachusetts does not appear to rise and fall with the level of CLEC foot traffic; the number has stayed constant at zero since CLECs began collocating in Verizon COs.

The record also contains no evidence that an increase in CLEC "foot traffic" causes an increase in other, non-network-affecting incidents. In response to a record request, Verizon provided a summary of incidents that were listed as security breaches by its security department or CCC. *See* Verizon Response to RR-DTE-VZ-2. This response lists 28 such incidents. Of these, seven (or one-fourth of the total) involved picketing or vandalism associated with the Verizon work stoppage in August 2000. Nearly all of the remaining incidents involved theft of or damage to CLEC equipment and cages. In none of these cases has Verizon identified the party responsible for the security breach. Thus, although Verizon's proposals rely on an assumed correlation between CLEC foot traffic and threats to network security, the record contains not a single documented case of any security breach, whether network-affecting or otherwise, attributable to a CLEC.

This is not surprising, given the importance of network integrity to CLECs. As Allegiance and other CLECs testified, the integrity of the network is just as important to CLECs as it is to Verizon. Exh. AL-1, at 5; Exh. Covad-1, at 17; Exh. Q-1, at 6; Exh. WCOM-1, at 11. If an accident or sabotage damages Verizon equipment, such damage can have a direct effect on

[3] Although relying on the concept to a high degree, Verizon never defines "foot traffic" nor any reliable measurement of "foot traffic." This is surprising given that the reduction of foot traffic seems to be the goal that drives Verizon's various proposals. One reason for the dearth of foot traffic data is that Verizon simply does not track the number or identity of people in its COs very effectively. Verizon's witnesses admitted that they have no way of telling, at any particular point, how many people might be in a particular CO and who those people are. Tr. 358-60. Verizon is, at most, capable of tracking who has entered a building where that building has a CRAS installed, but even then the system cannot tell who has left the building. *Id.* Verizon has installed CRAS in only 34 out of its 169 Massachusetts COs. Qwest-VZ-1-20.

CLEC equipment that may be interconnected to the Verizon equipment. Thus, CLECs and their employees have exactly the same incentive to safeguard the security and integrity of the network as do Verizon and its employees.

The Verizon witnesses took the position that CLECs and their employees pose a threat to network security because Verizon does not have direct control over the discipline and training of CLEC employees. Exh. VZ-MA-1, at 30-31. The evidence discussed above confirms that this argument is unfounded; despite being independent from Verizon, CLEC employees have not caused a single network-affecting incident in Massachusetts. In contrast, from 1999 through the present, Verizon has experienced seven network outages of sufficient magnitude to be reported to the FCC in the form of a service outage report. Six of these were caused by the actions of Verizon employees or vendors, while a seventh was caused by a water company. These incidents affected from 30,000 to as many as 2.8 million customers. *See* Verizon Response to RR-DTE-VZ-3, Att. 1. Allegiance does not contend that these incidents show that Verizon's employees are not well-trained or well-motivated. Rather, these incidents are simply further evidence that CLEC employees and vendors pose no greater threat to network security than do Verizon employees and vendors, and the Department has no basis for treating them in a vastly different manner, as Verizon recommends.

II. THE RECORD AND THE LAW DO NOT SUPPORT THE IMPLEMENTATION OF THE DRASTIC AND ANTI-COMPETITIVE MEASURES VERIZON PROPOSES.

Despite the lack of any evidence showing that the presence of CLECs in Verizon COs is a threat to network security, Verizon proposes measures that would drastically re-write the rules that govern colocation in Massachusetts. Most significantly, Verizon proposes to ban (1) the "commingling" of CLEC and Verizon equipment, meaning that one method of physical

colocation, CCOE, will be banned unless the equipment can be placed in separate and secure space; and (2) any type of physical colocation in COs found to be "critical" as determined by Verizon "working with the Department" to identify such COs. The implementation of either of these measures would be unlawful and utterly unsupported by credible evidence in the record.

A. Verizon's Two Main Proposals Are Unlawful Under The Telecommunications Act Of 1996 And The FCC Regulations Implementing The Act.

Verizon's two main proposals are a direct attack on CLECs' right to physical colocation as provided in the Act. The "critical CO" proposal would ban all physical colocation where Verizon sought to do so, based on criteria as yet to be determined. The "separate and secure only" proposal would ban one form of physical colocation, CCOE, where it results in "commingling" of CLEC and Verizon equipment (although it is that very feature of CCOE that makes it valuable in increasing the colocation capacity of a CO).

These measures would clearly be prohibited by current federal regulations, which Verizon itself recognizes. In its panel testimony, the witnesses discussed the effect of the FCC's colocation procedure regulations, set forth at 47 C.F.R. 51.323, which were promulgated in *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, CC Docket No. 98-147, Fourth Report and Order, FCC 01-204 (August 8, 2001)(*"Colocation Remand Order"*). Exh. VZ-MA-1, at 16. Verizon recognized that these regulations prevented ILECs from imposing harsh colocation restrictions, including the "separate and secure space only" and "separate entrance" requirements Verizon proposes here, on a blanket basis. Id. Verizon made much of the fact that these regulations were being appealed (by Verizon and other ILECs) and that the *Colocation Remand Order* "was released one month before the events of September 11th," apparently hoping that the D.C. Circuit would find its arguments more convincing after

September 11th than the FCC had found them before. This was not to be. On June 18, 2002, the D.C. Circuit denied Verizon's petition for review, leaving in place the FCC's rules regarding cageless colocation and the "separate space and entrance" requirements. *Verizon et al. v. FCC et al*, 292 F.3d 903 (D.C. Cir. 2002).

Implementation of Verizon's proposals would violate those rules. As the Department recognized in the Order opening this investigation, ILECs may restrict CLEC colocation to separate space and to construct separate entrances for CLEC personnel only in limited circumstances. *Order* at 5, *citing Colocation Remand Order.* In the *Colocation Remand Order* at para. 102, the FCC stated that

> "We therefore conclude that an incumbent LEC may require the separation of collocated equipment from its own equipment only if the proposed separated space is: (a) available in the same or a shorter time frame as non-separated space; (b) at a cost not materially higher than the cost of non-separated space; and (c) is comparable, from a technical and engineering standpoint, to non-separated space. We also conclude that an incumbent LEC may require such separation measures only where legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant them."

The FCC rejected, however, the idea that security concerns could justify imposing the "separate space and entrance requirement" as a blanket rule. "[T]here is simply insufficient evidence to support a finding that incumbent LECs' security concerns require physical separation of colocated equipment from the incumbent's own equipment in every instance." *Id*. at para. 101.

This is the very approach Verizon is taking in this case. It seeks to impose a "separate and secure" space and separate entrance requirement in each and every Massachusetts CO. In support of this proposal, Verizon cites no specific security concerns, only a general concern that "such measures will better protect the telecommunications network from harm in today's environment, as well as maximize safety and security for employees and agents of Verizon and

collocated carriers" (Exh. VZ-MA-1, at 5-6). In fact, Verizon admits that "there have been no verified security related incidents or breaches" at the one central office where a physical colocation would be converted to a virtual colocation arrangement as a result of Verizon's proposed "separate and secure" space requirement (Exh. AL-VZ-3-2), and there have been no security breaches attributable to CLEC personnel in any of the other 168 Massachusetts COs to which this new policy would be applied going forward.

In its prefiled Panel Testimony, Verizon's witnesses testified that it had appealed the FCC's *Colocation Remand Order* because it "effectively establishes a default rule that forecloses ILECs from requiring segregated space and separate entrances, thereby unduly interfering with the ILEC's fundamental right to manage effectively the use of its property and its obligations to protect the security of its telecommunications infrastructure and the safety of its employees." Exh. VZ-MA-1, at 16. At the hearings, Verizon witness Peter Shepherd explained Verizon's position in more detail. He testified that Verizon interpreted the FCC rules as allowing an ILEC to limit physical colocation where legitimate security concerns made physical colocation technically infeasible. Tr. 240-41. Mr. Shepherd's interpretation of "technically infeasible" is that segregated space is not available: "It comes down to space availability and security concerns." Tr. 241. This amounts, of course, to a blanket imposition of the space separation requirement. In Verizon's view, a CLEC can physically collocate only so long as there is segregated space available and, if there is not, "security concerns" demand that the CLEC be denied physical colocation.

This is the very position the D.C. Circuit rejected in its June 18, 2002 decision.[4] The

[4] The D.C. Circuit also rejected Verizon's even more extreme argument that a CLEC should be allowed to collocate only if it could prove that an off-site location was infeasible. *Id.* This argument was notable for its ignorance of the very language of the statute, which requires that a CLEC be given "access to unbundled network elements at the premises of the local exchange carrier." 47 U.S.C. § 251(c)(6).

Court of Appeals' discussion of Verizon's argument is most instructive, as it shows the lengths to which Verizon will go in fighting the Act's requirement that ILECs open their networks to competitors:

> This brings us, finally, to Verizon's challenge to the space assignment rules. According to Verizon, the "new rules, though superficially more limited" than the previous rules struck down in GTE, "nonetheless effectively allow competitors to insist on their space preferences and apparently prevent incumbents from requiring that competitors install their equipment in segregated space." Pet'rs' Opening Br. at 40. This argument lacks merit. Attempting to make the current rule resemble the vacated portions of the previous rule, Verizon mischaracterizes both. For example, Verizon states that "the default rule effectively remains what it was before: Incumbents apparently may not, as a general matter, require segregated collocation space and separate entrances." Pet'rs' Opening Br. at 40 (emphasis added). This inaccurately describes the Collocation Order; instead of mandating as a "default" that incumbents could not require segregated space and separate entrances, that order prohibited their use completely. See Collocation Order p 42.
>
> Turning to the current rule and mischaracterizing it as well, Verizon argues that ILECs' "security and efficiency concerns apparently count for nothing in the Commission's calculus." Pet'rs' Opening Br. at 41. The Commission, however, abandoned the requirement that CLECs be permitted to control the placement of equipment; rather, the Remand Order acknowledges that because "[a]n incumbent is far more familiar with the design and layout of its premises," it should have "ultimate responsibility" for determining where to place equipment. Remand Order p 90. Moreover, rather than banning separate entrances and segregated facilities outright, the Commission established a presumption against their use, which ILECs can rebut by showing that legitimate security concerns require separate facilities or entrances, that the separate facilities are comparable from an engineering stand-point, that they are available on a similar time frame, and that their use will not "materially" increase CLEC costs. Remand Order p 102. Finally, the Commission did not ignore ILEC security concerns; rather, it found "insufficient evidence to support a finding that [those] concerns require physical separation of collocated equipment from the incumbent's own equipment in every instance." Id. p 101.

Verizon et al. v. FCC et al., 292 F.3d at 907.

Not surprisingly, Verizon has a difficult time squaring this decision with its proposal to require separate space and separate entrances. When asked by Allegiance whether the D.C. Circuit's decision would have any impact on its witnesses' surrebuttal testimony, which

discussed the legality of its proposals, Verizon responded "No. See Verizon MA's Reply to AL-VZ 3-3." Exh. AL-VZ-3-7. Verizon responded to AL-VZ-3-3, however, by stating: "It is within the Department's scope of authority to determine whether physical colocation (including cageless colocation) is practical **in a given location**" (emphasis added). This answer shows that even Verizon recognizes that the Department cannot impose a blanket requirement of separate and secure space in every CO in Massachusetts, without some consideration of the actual conditions "in a given location." Evidence of what is practical in a given location, of course, is precisely what Verizon chose not to present in this case.

The D.C. Circuit's decision also renders pointless Verizon's request that the Department petition the FCC to change the rules that it finds so inconvenient. Petitioning the FCC to change these rules now would be a tremendous waste of time and resources, and would stigmatize Massachusetts as an unfriendly environment for telecommunications competition. This would be most ironic considering the importance of its telecommunications sector to the Massachusetts economy and the Department's role in setting the rules that have allowed that sector to flourish.

B. The "Critical CO" Measure Proposed By Verizon Is Unacceptably Vague And Designed To Deprive Affected CLECs Of Their Procedural Due Process Rights.

As part of its colocation security plan, Verizon proposes to work with the Department to identify those "critical" COs where virtual colocation only should be required. Exh. VZ-MA-1, at 39. Despite numerous discovery questions from intervenors regarding all aspects of its "critical CO" proposal, Verizon appeared determined throughout this proceeding to keep its "critical CO" plan as vague as possible.

As of the close of evidentiary hearings in this case, Verizon's "critical CO" plan remained vague in three critical areas. First, Verizon has failed to provide the Department or

CLECs with a list of specific COs which would be considered "critical" by Verizon or the specific number of colocated COs that might be deemed "critical COs" (Exh. XO-VZ-1-4). Second, Verizon has not provided a list of specific criteria which it proposes to employ to determine which colocated COs qualify as critical, and instead has provided only a list of possible, preliminary criteria (Exhs. XO-VZ-1-4; VZ-MA-1, at 39-40; VZ-MA-2, at 14-16). Third, and quite significantly, Verizon's suggested process for establishing which colocated COs will qualify as critical would exclude the very CLECs who would be most affected by any elimination of physical colocation, as Verizon has only offered vague references to working with the Department in some manner to determine which COs are "critical" and thus should be converted to virtual colocation only (Exhs. VZ-MA-1, at 39; AL-VZ-1-20 (Supp.)).

No single element of Verizon's vague "critical CO" plan is more troubling than Verizon's apparent willingness to "pick and choose" so-called "critical COs" without affected CLECs present. Although Verizon has asserted that it is up to the Department to "decide the appropriate forum in which to determine those central offices that would be considered 'critical' based on the sensitive nature of the information being evaluated" (Exh. AL-VZ-20 (Supp.)), up until now Verizon appears quite willing to move forward with its "critical CO" plan without the benefits of either adjudication or participation by affected interests.

This approach raises serious due process concerns. The Department recognized the significant interests at stake in this proceeding by conducting it as an adjudicatory proceeding, with the full G.L. c. 30A rights that accrue in such proceedings. *Order* at 7. The Department also granted all of the CLECs' petitions to intervene, which required a showing that a CLEC's interests would be "substantially and specifically affected" by the proceeding, as required by 220 CMR 1.03. Transcript, 2/25/02 Procedural Conference at 6-7; *Hearing Officer Memorandum*

Re: Procedural Schedule, Ground Rules, and Service List. Verizon would now like to bifurcate the proceeding so that the Department first approves the general concept that it may ban physical colocation entirely at certain COs, and then conducts a separate proceeding in private with Verizon to determine which COs meet the specific criteria set by the Department.

This approach would completely neuter the due process rights granted by G.L. c. 30A, and would be tantamount to allowing parties to participate only in preliminary, general matters rather than in the portions of a proceeding by which the parties would be "substantially and specifically affected." Having made the determination that CLECs have a substantial and specific interest in this proceeding, the Department must give proper notice and allow full participation, up to the point of any final orders, which an order banning CLECs from a particular CO certainly would be. *See CTC Communications*, D.T.E. 98-18-A (July 24, 1998) (reconsideration granted where Verizon given inadequate notice and opportunity to present evidence and argument before Department issued final order in the case).

In sum, Verizon's "critical CO" proposal is a substantive "black box" and a procedural star chamber that does not meet the minimum due process requirements of the Massachusetts APA. And, while Allegiance provides ample grounds below for the Department to reject Verizon's "critical CO" proposal on its merits, should the Department decide to consider further any aspect of Verizon's "critical CO" proposal, Chapter 30A of the General Laws and the basic tenets of due process would require the Department to consider Verizon's "critical CO" plan in a manner which allows those entities substantially and specifically affected by the plan to maintain the intervenor status already granted to them and to exercise all procedural rights accorded to such intervenors.

C. The Critical CO Plan Should Be Rejected On Its Merits.

1. The Evidentiary Record Does Not Support Adoption of Verizon's "Critical CO" Plan for Purposes of Security.

Even if the procedural defects in the process proposed by Verizon for selecting "critical COs" were cured, the proposal itself lacks merit and is not supported by evidence in the record. First, there is no evidence in the record that, even if "critical COs" could be identified, a blanket expulsion of CLECs from those COs would be justified by any improvement in security such a measure might bring. As has been the case with other aspects of its proposed colocation security plan, Verizon makes no effort to demonstrate that any of the COs which might be deemed critical[5] have ever experienced specific security problems caused by CLECs or others.

Moreover, other than arguing that "the increased number of additional personnel of other carriers accessing these locations, increases the opportunity or chance that inadvertent or intentional actions could harm those critical network facilities" (Exh. VZ-MA-2, at 14), Verizon did not establish that any security *benefit* would result from converting a CO to virtual colocation only. Verizon already implements a "separate and secure" physical colocation policy at its Massachusetts COs and the record of this proceeding indicates that there have been no significant CLEC-caused security breaches under this policy.[6] If CLEC employees presently are unable to access Verizon equipment and have not caused any system-affecting problems by virtue of working on their own equipment under current policy, what possible security benefit could be achieved by eliminating CLEC presence from "critical COs" altogether?

[5] Of course, Verizon offers very little information regarding how it might "work with the Department" to determine which COs qualify as critical under its proposal. However, even among Verizon's vague "preliminary" criteria for making such determinations, there is no mention of specific security concerns or experiences at specific COs.
[6] *See, supra,* at Section I.A.

In answering this particular question, Verizon repeatedly falls back on the argument that the greater the number of people in a CO, the greater the possibility of an accident or an incident. *See, e.g.*, Tr. 63, 117, 140, 157, 164; Exhs. VZ-MA-1, at 41; VZ-MA-2, at 2. This argument, like Verizon's entire colocation proposal, is blatantly anti-competitive, as it is premised on the unsupported assumption that Verizon employees, vendors and outside contractors are less likely than CLEC personnel to cause accidental or intentional damage to a CO. Of course, there is no basis in the record for this assumption. And, even if one were to determine that some unquantifiable security benefit could be gleaned from eliminating all CLEC foot traffic from so-called "critical COs", there certainly has been no showing by Verizon that any such benefit outweighs the significant costs to CLECs if all physical arrangements in those COs must be converted to virtual colocation. *See* Section II.C.4., below.

2. Verizon's Preliminary Proposed Criteria for Selecting "Critical COs" are Designed to Obtain Competitive Advantage, Not to Enhance Security.

What scant information Verizon has provided with respect to the criteria it would use to select "critical COs" indicates that its "critical CO" plan (1) is designed to deny CLECs physical access to the very COs that are most desirable to CLECs; and (2) has little to do with genuine concerns about security.

Even a cursory review of Verizon's preliminary criteria for selecting "critical COs" shows that Verizon's plan targets the COs where the most CLECs are likely to be colocated, making the anti-competitive effects of the proposal unacceptable. For example, the second preliminary criterion presented by Verizon for selecting "critical COs" is "the presence of critical customers" served by the CO (Exh. VZ-MA-1, at 39-40). And, while, as described below, Verizon did not answer legitimate discovery questions designed to elicit just which customers would qualify as "critical" under this criterion, it appears that, at a minimum, these customers

include major airports, military installations, government agencies and nuclear power plants, and, at most, include all of these customers *and* major businesses and advanced technology companies. Id., Exh. VZ-MA-2, at 14.

Of course, if the presence of major businesses and advanced technology companies is a contributing factor in determining whether a CO is "critical", then Verizon would have the means at hand to remove CLECs from truly "choice" COs, *i.e.*, the COs with the most attractive customers. Here again, even though Verizon has proposed the "critical CO" plan at issue in this proceeding and has placed its preliminary criteria for selecting such COs in evidence, Verizon proved unable to answer legitimate and direct questions regarding the scope of its own criterion.

For example, in its Panel Surrebuttal Testimony, Verizon stated that one of the factors governing which COs are "critical" is "whether accidental or intentional damage to the network resulting in disruption of existing service in particular central offices could….jeopardize the operations of major businesses, public safety, and government agencies, as well as advanced technology companies and other institutions that are involved in national security matters" (Exh. VZ-MA-2, at 14). Then, in response to a discovery question regarding whether these major businesses and advanced technology companies needed to be involved in "national security matters" in order to be a determining factor in deciding whether the CO that serves them is "critical" under Verizon's plan, Verizon appeared to confirm that some national security involvement was required. *See* Exh. AL-VZ-3-4. This confirmation, however, was soon contradicted by Verizon's witness, Mr. Shepherd, who testified that the criterion covered "businesses, government entities, public safety agencies, et cetera, that would constitute a significant impediment to the society or to the public's interest if communications for them were

lost" (Tr. 231), but who never stated that these businesses must have a national security function in order for the CO serving these business to be considered "critical."

In the end, Verizon's steadfast refusal to be pinned down with respect to the scope of its "major businesses" criterion is less important than the criterion itself. For, if Verizon is allowed to keep CLECs out of those COs which serve major businesses, then Verizon will have succeeded in implementing one of the most anti-competitive elements of its already anti-competitive colocation security proposal.

Another criterion suggested by Verizon to be used in classifying COs as "critical" is the presence of E911 tandems. However, the absence of any security breaches at COs with E911 tandems as well as the current lack of heightened security measures at COs with E911 tandems indicate that Verizon is less concerned with security, than with depriving CLECs physical access to their equipment in the most desirable COs.

In suggesting that the presence of E911 tandems (as well as other tandems and STP equipment) in a CO would be another factor to be considered in determining whether a CO is "critical", Verizon lays out some significant concerns. In its Panel Surrebuttal Testimony, Verizon's witnesses stated that the presence of an E911 tandem or an STP makes a CO critical:

> Because of the critical nature of the traffic they carry. By contrast to access tandems, neither an E911 control tandem nor a Signaling Transfer Point (STP) is a single point of failure in Verizon's network. In fact, both networks have been designed in a redundant fashion such that there is no significant single point of failure. Verizon designed its network this way because both networks are extremely critical to the network and public safety. There are four E911 control tandems in Massachusetts, and each central office is connected to two tandems. Even with this level of redundancy, accidental damage or a coordinated attack to one or more of these mated facilities has the potential to gravely disrupt emergency communications. Similarly, a coordinated attack on the mated Signaling Transfer Points (STPs) that serve a LATA has the capacity to discontinue all interoffice traffic in a LATA. Accordingly, security of E911 control tandems and STPs must be a high priority.

Exh. VZ-MA-2, at 15.

Allegiance concurs that security at E911 tandems is critical and must always be given a high priority. Based on the record of this case, however, it is not clear that Verizon provides heightened security at its COs with E911 tandems – either before September 11th or now. While Verizon raises the disturbing specter of a coordinated attack against one or more of the mated COs containing E911 tandems, it must be noted that the potential for this kind of attack did not begin with the filing of Verizon's colocation security plan in this proceeding. Nonetheless, even though three of the four COs housing E911 tandems are COs housing colocators (Exh. AL-VZ-3-5; AL-VZ-1-1, Att. 1), Verizon has never placed a security guard at any of these COs, despite the fact that Verizon's Security Department Manager agrees that security guards add a layer of security at Verizon's COs (Tr. 134).[7] Moreover, Verizon has not performed risk assessments at any of the three COs housing both E911 tandems and colocators (AL-VZ-RR-1).[8]

Like so many of the security proposals presented by Verizon in this docket, Verizon's preliminary proposal to eliminate physical colocation in COs with E911 tandems has little to do with security and everything to do with gaining competitive advantage. First, under Verizon's current "separate and secure" policy for physical colocation, the E911 tandems in Verizon's COs are located in secure space separate from CLEC colocation areas; CLEC personnel would need

[7] Further, Verizon has not deployed CRAS at its COs housing E911 tandems (Exh. Qwest-VZ-1-21).

[8] When Verizon's responses on cross-examination revealed that Verizon had done nothing to date to address security at three COs housing E911 tandems, Verizon's witness, Mr. Mattera, was quick to point out that these criteria were not "final criteria" and that Verizon had not yet identified its COs with E911 tandems as "virtual-only" offices (Tr. 154-155). Verizon, however, cannot have it both ways here. On the one hand, Verizon is attempting to offer as little information as possible as to which offices will be designated as "critical COs" under its plan, hoping instead to keep things as vague as possible until such time as it has its opportunity to "work" with the Department on these issues without the input of CLECs. On the other hand, when what little information Verizon has provided with respect to its plan proves to undercut the credibility of Verizon's security objectives, Verizon attempts to argue that this information was not final anyway.

key or card access to come in contact with these tandems (Exh. AL-VZ-3-5). Second, Verizon has presented no evidence that there have been any security problems up to now at these COs. Third, Verizon has not seen fit to either evaluate security (through the performance of risk assessments) or beef up security (by assigning security guards) at COs with E911 tandems. Yet, despite the absence of security problems at these COs and the lack of any security initiatives by Verizon at these COs, Verizon asks the Department to eliminate CLECs' physical presence at these COs altogether. In Allegiance's view, Verizon's proposal with respect to COs housing E911 tandems is designed primarily to deny CLECs the most efficient and cost effective means of interconnecting and accessing unbundled network elements and, like all other elements of Verizon's April 5, 2002 colocation security proposal, should be summarily rejected by the Department.

3. The Department Should Not Be Assuaged by Verizon's Contention that Only a "Handful" of COs Would Be Designated as Critical Under its Proposal.

Moreover, the Department should not be assuaged by Verizon's position that only a "handful" of COs ultimately would be designated as "critical" and converted to virtual colocation (*See* Exh. VZ-MA-1, at 40). First, despite numerous requests for specific information regarding the COs which might be affected by this proposal, Verizon has provided no list of such COs. Absent a verifiable list of "critical COs" (or, at least, "proposed critical COs") from Verizon, the Department should not accept Verizon's unsubstantiated view that only a few or a "handful" of COs will qualify as "critical".

Second, the record in this proceeding belies Verizon's assertion that only a "handful" of colocated COs would be converted to virtual colocation under its "critical CO" plan. If Verizon is allowed to employ the preliminary criteria for selecting "critical COs" which it has presented to the Department in this case, far more than a "handful" of COs would be converted to

colocation only. For example, Verizon suggests that the presence of a tandem switch, an E911 tandem switch, and/or STP equipment – equipment which Verizon characterizes as "the lifeline to numerous subtending switches throughout Massachusetts" – be used as a criterion in determining which COs are designated as "critical" (Exh. VZ-MA-1, at 40). But, by Verizon's own admission, the application of this criterion alone would result in far more than a "handful" of COs being designated as "critical" under Verizon's plan. Specifically, the "Description of the Basic Network Components" appended to Verizon's Panel Testimony notes that "many of Verizon's COs contain emergency 911 ("E911") switches and adjunct equipment" (Exh. VZ-MA-1, Att. 3, at 2), a statement which is entirely at odds with Verizon's assertion that only a "handful" of COs will be designated as critical if its "critical CO" proposal is allowed.[9]

Third, Verizon's "critical CO" proposal would be unacceptable even if only a "handful" of COs would be converted to virtual colocation as a result of its implementation. Where Verizon's "critical CO" proposal is vague, unnecessary, without benefit, and discriminatory, there would be no reason to convert a single colocated CO to virtual colocation as a result of this plan. As discussed further below, the problems associated with virtual colocation are so significant that CLECs' ability to provide timely and competitive service to their customers would be adversely impacted. The cost and competitive implications of eliminating physical colocation – even in only one CO – warrant rejection of Verizon's "critical CO" plan.

[9] Similarly, as discussed in Section II.C.2., above, to the extent that Verizon's criteria for designating COs as "critical" includes a factor by which COs serving major businesses and advanced technology companies are deemed "critical", Allegiance is hard pressed to understand how only a "handful" of COs ultimately would be designated as "critical" once Verizon's criteria are applied.

4. Because Virtual Colocation is an Unacceptable Alternative for CLECs, Adoption of Verizon's "Critical CO" Plan Would Result in A Significant Diminution of Competition.

Finally, there is evidence in the record that virtual colocation is not a viable alternative to physical colocation, and that some CLECs would consider abandoning any CO rather than attempt to use virtual arrangements in place of the physical arrangements they designed, purchased and installed in reliance on continued 24-hour physical access to that equipment.

Allegiance's witness in this proceeding testified with respect to Allegiance's poor experience with virtual builds in Verizon territory in New York, New Jersey and Pennsylvania (Exh. AL-1, at 9; Tr. 428-429). Other CLECs presented evidence showing similar problems with virtual colocation generally and specifically in Verizon territories (Exhs. WCOM-1, at 9-10; ATT-1, at 17; Covad-1, at 7-10; Covad response to Verizon 1-5). Virtual colocation requires CLECs to be completely dependent on ILECs for both necessary maintenance and repair of equipment. In Allegiance's case, Verizon response time for maintenance and delivery in virtual colocation arrangements has been poor (Exh. VZ-AL-1-11). In addition, Allegiance has experienced problems in both establishing new virtual colocations in Verizon central offices in other states and adding to its virtual colocation arrangements (Exh. AL-1, at 9).

With respect to new virtual colocation arrangements in other Verizon states, Allegiance has experienced consistent delays. These delays have resulted because the limited list of vendors that Verizon has approved for installation work were constantly booked and unavailable; Verizon limited the number of access trips Allegiance project managers could make to monitor progress of these builds; the work performed by approved vendors was not always good and last-minute rebuilds were required on several occasions; and Verizon-controlled inspections were often delayed. These delays, of course, are significant when CLECs are unable to timely implement customer orders and begin generating revenue. Exh. AL-1, at 9-10.

Most significantly, as a result of its experiences with virtual colocation in other states, Allegiance has not added any new virtual colocations in the Verizon region since March 2000. Id. at 10. And, while it may be the case that Allegiance's poor experience with virtual colocation has taken place in the Verizon region outside of Massachusetts, Verizon has not been able to establish in this proceeding that its processes and procedures for installing, inspecting, maintaining and repairing CLEC equipment in virtual colocation arrangements are any different in Massachusetts than in other Verizon states.

Moreover, Allegiance's witness, Wendy Perrott, testified that if the Department accepts Verizon's proposal to convert its physical colocation arrangements in so-called "critical COs" to virtual colocation only, Allegiance may not be able to maintain the arrangements and relationships it has with customers it serves out of those COs (Tr. 423). This is true for two reasons. First, as Ms. Perrott pointed out in the hearings, Allegiance uses third-party fiber in many of its Massachusetts colocations which allows for more efficient and less costly service to customers (Tr. 422). The ability to use third-party fiber and the "hubbing" of multiple COs that fiber connections allows depends upon Allegiance having both physical colocations and around-the-clock access to those physical colocations. Id. Allegiance already has its physical equipment and fiber in place for its Massachusetts colocations, and conversion of any of those physical colocations to virtual would fundamentally disrupt Allegiance's network architecture.

Second, like many CLECs, Allegiance provides DSL services to its customers through physical colocations. Allegiance does not provide DSL through virtual colocations because of the technical limitations of that arrangement and the maintenance required to offer high-quality DSL which, again, depends upon around-the-clock access to physical colocations (Tr. 423). Conversion to virtual colocation at a "critical" CO would require Allegiance to discontinue its

DSL service to customers served from that CO.[10] Simply put, the inability to access colocated equipment on an as-needed basis for line testing, maintenance and repair purposes would significantly diminish the ability of CLECs provide timely and high quality service to their customers.

D. A Compromise Plan That Would Not Require Virtual Colocation Only At "Critical COs", But Instead Would Require Scheduled Escorts For CLEC Visits To Separate And Secure Space In Such COs, Presents Unacceptable Cost And Technical Problems For CLECs.

In the course of evidentiary hearings in this proceeding, Department staff asked a number of CLEC witnesses to comment on an alternative "critical CO" plan where designated COs would not be converted to virtual colocation only, but instead CLEC personnel would be able to access equipment in these COs only when accompanied by 24X7 escorts. For the reasons set forth below, the Department should not consider this alternative proposal further.

First, as Allegiance's witness testified, the escort requirement would cause Allegiance to incur additional and unbudgeted costs – both in terms of any escort charge and the costs associated with taking Allegiance technicians away from servicing customers to coordinate instead with Verizon escorts (Tr. 423-428). Second, as WorldCom's witness testified, the problems associated with coordinating with an escort would make it difficult for that CLEC to maintain its service-level agreements (Tr. 514-516).

Finally, AT&T's witness pointed out that even if an escort is theoretically available 24 hours a day, seven days a week, that does not necessarily translate to 100% availability (*See* Tr. 474).

[10] In addition, two other CLECs, Covad Communications and WorldCom, testified that conversion of its physical colocation arrangements to virtual colocation would render these CLECs unable to maintain their service level agreements with customers (Tr. 513-516, 559).

In the end, based on the record of this proceeding, Verizon has not established that any security issues exist which warrant the implementation of any element of its proposed colocation security plan. Moreover, the record shows that Verizon's security proposal is designed more to deny CLECs their statutory rights to colocation than to enhance security at its COs. For these reasons, the Department should not adopt a "compromise" escort requirement in so-called "critical COs" or otherwise strive to find some "middle ground" whereby CLECs are somewhat limited – but not fully limited – in accessing their physical colocations. Absent any security problems or demonstrated security benefits from these alternative plans there is no justification for settling on a "middle ground" where CLECs' costs are increased, CLECs' rights are decreased, and customers end up with the "short end of the stick."

CONCLUSION

The Department opened this investigation in a sincere attempt to assess the current state of security at Verizon central offices and other facilities. Every party to this proceeding, from Verizon to every CLEC to the workers represented by the IBEW, has the same incentive to protect those facilities and the equipment and personnel they house. Rather than address security concerns openly and honestly, Verizon has used this proceeding as yet another skirmish in its ongoing war against allowing CLECs into its COs. That approach does nothing to further the legitimate goal of improving CO security in a manner that does not unnecessarily hamper competition. Verizon's recommendations seem intended only to adversely affect competition, without any demonstrable increase in security, which is why such proposals as the "separate and secure space only" rule continue to be rejected by the FCC and the Federal courts. The citizens

of Massachusetts deserve better than what Verizon offers. Allegiance urges the Department to reject Verizon's proposed changes to colocation security policies in their entirety.

Respectfully submitted,

ALLEGIANCE TELECOM OF MASSACHUSETTS, INC.

By its attorneys

_____

Robert D. Shapiro
Christopher H. Kallaher
Rubin and Rudman LLP
50 Rowes Wharf
Boston, MA 02110
Tel. No. (617) 330-7000

_____

Mary C. Albert
Vice President, Regulatory and Interconnection
Allegiance Telecom, Inc.
1919 M Street, N.W., Suite 420
Washington, DC 20036

Dated: August 9, 2002