COMMONWEALTH OF MASSACHUSETTS
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department on its own motion, pursuant to G.L. c. 159, §§ 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts	D.T.E. 02-8

INITIAL BRIEF OF AT&T COMMUNICATIONS OF NEW ENGLAND, INC.

AT&T COMMUNICATIONS OF NEW ENGLAND, INC.

Jeffrey F. Jones, Esq
Kenneth W. Salinger, Esq.
Jay E. Gruber, Esq.
John T. Bennett, Esq.
Palmer & Dodge LLP
111 Huntington Avenue
Boston, MA 02199-7613
(617) 239-0449 (voice)
(617) 227-4420 (fax)

Philip S. Shapiro
AT&T Corp.
111 Washington Avenue, Suite 706
Albany, NY 12210-2213
(518) 463-3148 (voice)
(518) 463-5943 (fax)

August 9, 2002

TABLE OF CONTENTS

Introduction

The Department opened this proceeding "to examine the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts ("Verizon") in light of heightened security concerns after the events of September 11, 2001." (*Vote And Order To Open Investigation*), D.T.E. 02-8 January 24, 2002, at 1. The record of this proceeding conclusively demonstrates that no collocation policy changes are needed to address the risks of terrorism that have been identified since September 11, 2001. Common sense security improvements, rather than drastic changes in collocation rules, are more than adequate to address Verizon's concerns in this docket.

A systematic approach to the Department's question involves the following logical analysis:

- ? ? What risks have arisen since September 11th, and what, if any connection is there between those new risks and collocation?
- ? ? If there are any identifiable risks to collocation security, what are the most cost-effective and least burdensome means of addressing them?
- ? ? Is a change in collocation rules the most cost-effective and least burdensome means of addressing them?

Unfortunately, Verizon has not taken the Department's question seriously. Instead of proceeding logically with an identification of the risks and a determination of whether collocation rule changes are the most cost-effective means of addressing them, Verizon has used the occasion of the Department's institution of this proceeding to advance Verizon's long standing objective, pursued for competitive advantage, of undercutting the right of competitive local exchange carriers ("CLECs") to physically collocate in Verizon central offices. As a result, much of the substantial expense of this docket has been largely wasted on a proposal that is unrelated to

legitimate security concerns, and opportunities for consensus and progress have been displaced by commercial maneuvering for competitive advantage.

Verizon's opportunistic approach to this docket is unfortunate for the further reason that Verizon has hampered the development of an appropriate record. As the owner and manager of its central office buildings, Verizon was well positioned to offer a reasoned analysis of the risks to which it is subject, risks that even Verizon admits in this proceeding must be identified on a site-by-site basis. Tr. 1, at 24 (Craft). Yet, Verizon declined to conduct any risk assessment, on a site-specific basis or otherwise. Tr. 1, at 39-40 (Craft). In its capacity of owner and manager, Verizon was also well positioned to collect data from which different levels of risk could be assessed and measures to address them developed. Yet, Verizon declined to do so, instead leaving it to the other parties to request the data and seek to make some sense out of it.

As demonstrated below, the record in this case is rife with Verizon's double speak and double standards. Verizon's on-again, off-again use of cost/benefit analysis is just one example. On the one hand, Verizon witness Peter Shepherd claims that it is not appropriate to engage in a cost/benefit analysis. Exh. AL-VZ 1-23. On the other, Verizon witness Lawrence Craft testifies that a cost/benefit analysis is an important aspect of determining appropriate security measures. Tr. 1, at 24-25 (Craft). On the one hand, the cost and business disruption of eliminating physical collocation entirely from central offices was not considered when Verizon made its "virtual collocation only" proposal. Tr. 1, at 46, line 5 (Craft). On the other hand, cost and business inconvenience is a reason that Verizon does not add a simple "anti-passback feature" to its existing electronic card reader system. Exh. VZ MA-2, at 24. Quite simply, no reasoned analysis and indeed no meaningful evidence supports Verizon's radical proposals.

In addition to the fallacies and omissions of Verizon's case, two major points are clear from the record. The first is that there is no nexus between the new risks of terrorism that have been identified since September 11th and collocation rules. In that regard, AT&T's witness panel, including AT&T's world class security expert, Michael Paszynksy, stated succinctly:

> To the extent that this proceeding has been initiated to examine risks not previously addressed when the existing collocation rules were put in place, there is little that an adjustment to these rules could accomplish. The new security risks that have materialized of late, namely organized terrorist threats, cannot be properly addressed through a change in collocation policy.

Exh. ATT-1, at 9.

The second point relates to a method, and possible result, for addressing the risks that collocation rules might reasonably address. In that regard, AT&T's panel stated:

> It is, of course, always possible to increase the level of security. However, increasing levels of security come with increasing costs -- both visible costs, such as new construction and equipment costs, and less visible costs, such as operational inefficiencies and impairment of competition.
>
> Any security plan must recognize the expense and inconvenience associated with certain measures. After analyzing the risks facing telecommunications facilities in Massachusetts, it is necessary to determine how much inconvenience is warranted and what level of cost is appropriate. It is necessary, therefore, to determine the point at which increasingly costly security measures provide such a small improvement to actual security, that it is no longer worth the cost. It is simply not possible to decide whether there is sufficient "security" in the abstract, because we can never achieve complete and perfect security.
>
> Any determination of the appropriate type of collocation arrangements for achieving "adequate" security must necessarily balance the cost of changing the existing collocation arrangements (which were determined to be optimal prior to concerns raised by the September 11th terrorist attacks) against the benefits such increased security measures produce. Moreover, where increased security can be achieved through measures that do not involve significant changes to previously determined collocation arrangements and that do not interfere with important policy goals -- such as the development of competition -- those measures should be used instead of costly, anti-competitive alternatives.

Exh. ATT-1, at 5.

Applying a reasoned method to the hard evidence of the limited security issues revealed in this case, the following cost-effective and minimally disruptive modifications to Verizon's security procedures would be appropriate:

1. Improvements to Verizon's method for recording and analyzing "security" violations;

2. Improvements to Verizon's method for communicating with CLECS regarding security matters;

3. More frequent background checks; and

4. Deployment of Card Reader Access Systems ("CRAS") with anti-passback features.

Summary Of Verizon's Proposal

Verizon's proposal in this case is remarkable in two major respects. First, if the new risks are so great as to warrant the radical change in collocation rules recommended by Verizon, it is unclear why Verizon has waited to make this proposal until a state commission has raised questions regarding collocation. Moreover, it is unclear why Verizon has chosen to make such a proposal in only one state, rather than at the FCC. If such concerns were real, addressing them should not depend merely upon procedural opportunity.

Second, Verizon's proposal is remarkable for its ambiguity. Verizon begins by identifying the following measures that it contends are "additional security measures [that] Verizon MA propose[s] in this proceeding for its collocated sites in Massachusetts" (Exh. VZ MA-1, at 23, lines 16-17):

> (1) establishing, for all forms of physical collocation (caged and cageless) separate space (e.g., separate rooms, floors, entrances and/or pathways to such areas) that secures and segregates collocators' equipment from Verizon MA's network facilities and prevents the commingling of collocators' equipment in the same areas as Verizon MA's equipment on an unseparated or unsecured basis;

> (2) relocating existing unsecured CCOE arrangements to secured, separated areas, where space permits, or otherwise converting them to virtual collocation arrangements;
>
> (3) providing CLECs with reasonable access to shared facilities outside the secured and segregated collocation space where partitioning of Verizon MA's equipment is feasible;
>
> (4) providing either virtual collocation and/or escorts for CRTEE arrangements; and
>
> (5) converting existing physical collocation arrangements to virtual collocation in selected, highly sensitive security risk COs.

Exh. VZ MA-1, at 23-24. Yet, when pressed for clarification, Verizon explained that, apart from the "virtual collocation only" proposal (#5), Verizon's proposal does not represent a change from current "practices." Exh. VZ MA-2, at 7, lines 21-23. Verizon states that "the other four requirements are *for the most* part already in place and followed today in Massachusetts." *Id.* (emphasis added). Verizon then cryptically notes that its "collocation security proposal would retain many of Verizon MA's current policies, and further enhance them as described in our previous testimony[.]" *Id.*, at 7-8.

With respect to the first and second items of Verizon's proposal, Verizon explains that it means, by these items, that all central offices should be constructed so as to permit CLECs access to their own equipment without having access to areas in which Verizon equipment is located. Exh. VZ MA-2, at 8-9. Verizon further states that all Massachusetts central offices are currently so constructed (*i.e.*, have separate pathways leading to CLEC equipment and have the CLEC area separate from Verizon's equipment), with the exception of the Hopkinton central office, where the building configuration does not permit construction of a separated collocation area. Exh. VZ MA-2, at 8-9. The net effect of the first and second items of Verizon's proposal, therefore, appears to be as follows. The one in-service arrangement in Hopkinton would be converted to virtual collocation, and Verizon would have "the ability to close a central office to

physical collocation if secured segregated space cannot technically be made available" (Exh. VZ MA-2, at 10, lines 12-13), an ability that Verizon does not currently have. Indeed, as discussed below, the ability that Verizon seeks is not presently permitted under federal law.

With respect to the third item of Verizon's proposal, which relates to CLEC access to common areas, Verizon appears to be asking for the Department's approval of a requirement that Verizon has been imposing on CLECs without prior Department approval: "coordinated, pre-arranged access at the carrier's expense for access to temporary staging areas, loading docks, freight elevators or exterior building openings for rigging and vendor equipment deliveries, etc." Exh. VZ MA 2, at 11, lines 5-8. Verizon is also asking that the Department approve a new restriction. "[I]f Verizon MA cannot provide secured access to common areas (*e.g.*, restrooms), the collocated carrier personnel should not be permitted to traverse Verizon MA's equipment areas to reach that facility." Exh. VZ MA 2, at 11, lines 12-15. Apparently, Verizon is asking the Department for the right to deny to CLEC technicians working in a collocation cage the right to use the restroom in a Verizon central office in certain situations, at least not without the use of an escort. Tr. 2, at 466, lines 3-5 (Nurse).

With respect to the fourth item (providing either virtual collocation and/or escorts for CRTEE arrangements), Verizon's proposal would require CLECs either to virtually collocate equipment at remote terminals or to obtain escorts to service their own equipment. Verizon appears to characterize this as constituting no change simply because there are no CLECs which have collocation arrangements at remote terminals at the moment. Such approval of Verizon's proposed fourth item, however, would constitute a change from the Department's present rules regarding collocation at remote terminals. *See* VZ Tariff No. 17, Part E, Section 11.1.5.

The fifth item, by Verizon's own admission, constitutes a radical departure from present collocation policy and rules. Here, Verizon is proposing that physical collocation be prohibited altogether in certain, so-called "critical" central offices. VZ MA Exh. 1, at 39. Verizon's proposal, however, does not specify which central offices would be considered "critical." Verizon suggests certain factors for determining whether a central office would be considered "critical," such as the number of access lines served by the office, the potential for national security risks, impact on health, safety and welfare, impact on businesses, and public safety and government agencies. *Id.* The factors that Verizon proposes to be used are not objective and not easily applied. Verizon was evasive as to the proportion or number of central offices that would fall under its proposed criteria. Verizon could not even exclude the possibility that all of its central offices would fall within its proposed criteria. Tr. 1, at 83-84 (Reney).

Indeed, Verizon does not even contend that factors it now suggests should be the specific ones that the Department considers and approves. Tr. 1, at 84, line 20 (Shepherd). Verizon proposes only that the Department conduct further proceedings to determine what those factors should be, and then which central offices satisfy those factors and provide CLECs with virtual collocation only. *Id.* Given the possibility under Verizon's rather loose proposal that no central offices would satisfy the factors, or that all central offices would satisfy the factors, it is not clear whether Verizon has made a proposal at all.

Argument

I. CONCERNS OF TERRORISM IN THE WAKE OF SEPTEMBER 11TH DO NOT WARRANT A CHANGE IN COLLOCATION RULES.

As mentioned above, this investigation was opened by the Department to explore potential deficiencies in collocation security in the wake of the terrorist attacks of September 11, 2001. Thus, this investigation is meant to examine whether terrorism presents a threat to the

integrity of the Massachusetts telecommunications infrastructure, and whether a change in collocation rules is necessary to combat such a threat.

No party to this proceeding has established that the Massachusetts telecommunications network faces a threat of physical terrorism akin to the events of September 11th, or that if it did, changes in collocation policy would be effective in lessening such a risk. While much speculation abounds as to the level of terrorist interest in various public utility targets, no party has been able to point to any evidence that the Massachusetts network is at physical risk from terrorism. Attacks upon telecommunications facilities simply do not provide terrorists with the kind of public exposure that attacks upon other civilian targets create. Exh. ATT-1, at 18-19. The very goal of terrorism is to inspire fear among the general population. Exh. ATT-1, at 8-9. This is most dramatically and effectively produced by attacks that put everyday citizens in immediate physical danger. An attack upon a power plant that pitches a major city into a blackout accomplishes this goal. Poisoning a metropolitan water system to strike thousands with severe illness accomplishes this goal. Such events lend themselves to massive press coverage and widespread public concern. Exh. ATT-1, at 8-9. A physical attack upon a central office simply does not accomplish this effect. *Id.*

The likelihood of physical harm to the network is further reduced when one examines terrorists' other options. Many security experts agree that the more profound terrorism threat is "cyber-terrorism", i.e., an electronic attack upon the "engines" running telecommunications, power, water, emergency services, air traffic control and the like from a remote location. Exh. VZ-ATT 1-1, *see also* Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, Wash. Post, June 27, 2002, at A1. This method of attack would undoubtedly be more attractive to a terrorist given that it accomplishes the same goal as a physical attack, but does so anonymously. Exh. ATT-1,

at 8, lines 19-21. Terrorists hacking into the telecommunications network from a remote location do not face the same risk of capture that a terrorist carrying out a physical attack would face. Such an attack may also have a wider impact, potentially disrupting an entire regional or national network rather than a single central office. Exh. VZ-ATT 1-1. Simply put, a cyber-attack achieves maximum gain with minimum exposure, clearly an option superior to physical attack.

Understandably, the Department may be unwilling to wait for the development of a clear evidence of terrorist plots to do physical harm to the network before deciding to act in this proceeding. Terrorist cells, after all, are not in the habit of publishing their target lists. Yet, the Department should act with due care in this case. Based upon the recent history of terrorist activity, a physical attack upon a telecommunications facility seems exceedingly remote. This should be taken into account when considering any security measure that would prove costly and disruptive to users of the network, such as a radical change in collocation rules.

The evidence of "security breaches" produced by Verizon in this proceeding makes clear that the physical collocation of CLECs has not raised the potential for physical harm to the network in Massachusetts. Exh. AG-VZ 1-1. Indeed, it is entirely possible that CLECs are the predominant victim of the security incidents Verizon has produced in this proceeding. Tr. 2, at 453-54 (Nurse). In any event, since the inception of physical collocation in Massachusetts central offices, not a single reportable service disruption has been caused by CLEC personnel in the central office. Tr. 1, at 58, line 12 (Craft); Exh. AG-VZ 1-1. Moreover, reducing the presence of CLECs in central offices would likely *worsen* the quality of any response to a potential physical attack upon a central office. AT&T witness Tony Fea, who managed the company's restoration of service in Manhattan following the September 11th attack, testified that removing the CLEC presence from Verizon's West St. central office would have delayed

restoration efforts. Tr. 2, at 451-52 (Fea). Since CLECs had equipment in the facility and technicians available to service that equipment, more manpower and expertise were brought to bear on the problem than would have been available if Verizon were the sole occupant of the facility.

The record supports the following conclusions. Telecommunications facilities in Massachusetts face a comparatively low risk of terrorist attack. Physical collocation does not exacerbate whatever risks do exist. The lack of collocation, in fact, may worsen certain aspects of a terrorist attack such as the quality of the service response to such an incident. Given these factors, the Department should take a conservative approach to any changes in the collocation regime.

II. THE DEPARTMENT SHOULD REJECT VERIZON'S PROPOSED COLLOCATION RULE CHANGES BECAUSE THEY ARE UNSUPPORTED BY ANY RISK ASSESSMENT OR REASONED APPROACH.

A. AN APPROPRIATE RISK ASSESSMENT AND ASSESSMENT OF COSTS MUST BE DONE IN ORDER TO DETERMINE WHETHER, AND WHAT TYPES OF, SECURITY MEASURES SHOULD BE IMPLEMENTED.

A risk assessment involves the identification of risks associated with a particular facility. Tr. 1, at 23 (Craft). *See also*, Exh. ATT-1, at 6, 9-10. As such, there can be no generic risk assessment for all collocated facilities. There is no dispute in this proceeding among the parties that risk assessments are an important part of the process for determining whether additional security measures are warranted and, if so, what type of security measures are warranted. Tr. 1, at 24, lines 4-8 (Craft); Exh. ATT-1, at 5 . Indeed, Verizon's security expert, Mr. Craft, testified that, after a baseline level of security is achieved, a risk assessment is required to determine the amount of additional security that is warranted. Tr. 1, at 24, lines 13-18. There is also no dispute in this proceeding among security experts that, in order to determine whether additional security measures are warranted, there needs to be a comparison of the costs associated with the

implementation of the security measures, with the benefits achieved by the security measures. Tr. 1, at 25, lines 6-13 (Craft). *See also*, Tr. 1, at 40, lines 16-22 (Craft); Exh. ATT-1, at 5, lines 15-19.

There is even agreement on the categories of costs that are to be considered when determining whether additional security measures are warranted. Those costs include not only the out-of-pocket, financial costs of implementing additional security measures, but also costs associated with business disruption and inconvenience, and decreases in business efficiency. Tr. 1, at 25, lines 14-23 (Craft); Tr. 1, at 45, lines 18-23 (Craft); Exh. ATT-1, at 5. Indeed, all negative impacts on non-security concerns should be considered in an appropriate cost-benefit analysis. Tr. 1, at 25, line 20, through 26, line 3 (Craft); Exh. ATT-1, at 5. Such negative impacts necessarily include any detrimental effects on the implementation of important public policy goals, such as the promotion of competition in the local exchange market. Exh. VZ-ATT 1-4.

In order to compare the costs of security measures to their benefits, the benefits must be assessed and quantified to the extent possible. There is even broad agreement as to an approach for determining the benefits. The benefits are, of course, the harm to the network that is prevented by the implementation of additional security measures. *See, generally*, Tr. 1, at 40, line 23 through 41, line 3 (Craft). There are at least two dimensions associated with the quantification of that harm. They are the extent of harm, should it occur, and the likelihood of its occurrence. Tr. 1, at 45, lines 8-14 (Craft).

In sum, the security experts agree: there is a way to determine whether additional security measures at Verizon's central offices are warranted, what they are, and whether changes in collocation rules are required. Yet, in making its proposal to the Department in this docket,

Verizon ignored this undisputed and well established approach for addressing the Department's question regarding security and collocation. Indeed, Verizon ignored the approach that Verizon's security expert whole-heartedly endorsed on the stand under oath. Instead, as explained in detail below, Verizon cynically used the Department's question as an opportunity to resurrect its long-standing and anticompetitive position that CLECs should be excluded from Verizon central offices.

B. RATHER THAN PERFORMING A RISK ASSESSMENT, VERIZON USED THE OPPORTUNITY THAT THIS DOCKET PRESENTED TO PRESS ITS LONG-STANDING POSITION AGAINST PHYSICAL COLLOCATION IN AN EFFORT TO OBTAIN COMPETITIVE ADVANTAGE.

1. Verizon's Proposal Fails To Engage In The Risk Analysis Recommended By Its Own Expert.

Significantly, Verizon failed to provide to the Department in this case a single aspect of the risk assessment and analysis that its own security expert testified under oath should be done before additional security measures are adopted. After testifying that a risk assessment should be performed in order to determine whether, and what type of, additional security measures are warranted in Verizon's central offices, Verizon's security expert conceded that Verizon did not present to the Department any risk assessment, much less one that supports its "virtual collocation only" proposal. Tr. 1, at 40, line 4 (Craft); RR-IBEW-VZ 1. After testifying that the potential harm, including the likelihood of its occurrence, should be analyzed, Verizon's security expert conceded that no such analysis had been done. Tr. 1, at 45, lines 6-17. After testifying that business disruption and increased business inefficiencies should be taken into account, Verizon's security expert conceded that no such analysis had been performed in support of Verizon's proposal. Tr. 1, at 45, line 17, through 46, line 5. Indeed, after admitting that business disruption and inconvenience are valid considerations, Mr. Craft was forced to concede that Verizon, in developing its proposal, did not even consult with CLECs to determine the extent of

business disruption, inconvenience and increased inefficiency that might result. Tr. 1, at 46, lines 6 through 18. Mr. Craft further admitted that Verizon had conducted no analysis that would support a conclusion that CLEC operations would not be adversely affected by his proposal. Tr. 1, at 47, lines 3-7. After testifying that risk assessments must be performed on a site-by-site basis, Verizon's security expert admitted that no site specific analyses had been performed. Tr. 1, at 24, lines 2-3 (Craft).

One of Verizon's omissions is especially telling, because it illustrates why Verizon did not engage in any analysis. After stating that the likelihood of a risk actually occurring should be estimated, Verizon's security expert admitted that no such analysis had been performed. Tr. 1, at 45, lines 12-16. Such an omission is especially egregious because Verizon had data that would permit it to perform such an analysis. Specifically, Verizon had data from which it could determine the likelihood of a network outage resulting from the collocation "risks" that it had alleged. Verizon identified the incidents that purportedly represent security collocation risks caused by in Exh. AG-VZ-1-1. It is a simple matter to estimate the likelihood that those risks will produce a network outage. Such an estimate could be obtained by dividing the number of network outages that resulted from those incidents by the number of incidents. Tr. 1, at 57-58. Verizon apparently declined to perform such an analysis because there were no network outages that resulted from any of the collocation incidents identified by Verizon as a risk. Tr. 1, at 58, lines 8-12. (This should be compared to the number of reportable network outages caused by Verizon employees: six out of seven; the seventh was caused by a water company. RR-DTE-VZ-3.)

Given the complete absence of the very support Verizon's own expert states should be provided, the Department should reject Verizon's proposal outright.

2. Rather Than Identifying New Risks, Verizon Used The Opportunity Presented By This Docket To Advocate A Long-Standing Position That Has Been Rejected Many Times By Both The FCC And The Department.

Instead of following these fundamental and reasonable methods of analysis, Verizon has chosen to use this proceeding to dredge up tired arguments against physical collocation that have been long rejected by the FCC and the Department. As detailed in Section III below, the Telecommunications Act of 1996 made it a statutory requirement for ILECs to provide "for physical collocation of equipment necessary for interconnection or access to unbundled network elements at the premises of the [LEC]. . ." 47 U.S.C. § 251(c)(6). The statute permits only two exceptions to this requirement, where the ILEC is able to demonstrate that "physical collocation is not practical for technical reasons or because of space limitations." 47 U.S.C. § 251(c)(6). In its *First Local Competition Order*, the FCC recognized that ILECs "have the incentive and capability to impede competitive entry by minimizing the amount of space that is available for collocation by competitors." *First Local Competition Order* at ¶ 585.

The Department has recognized this danger to competition as well. In its *Teleport Petition* decision, the Department specifically reiterated the FCC's findings in its *First Local Competition Order* and *Advanced Services Order*, stating that ILECs had major incentives to delay the provision of physical collocation due to competitive interests. *See* D.T.E. 98-58 Order (July 30, 1999) at 13-14. The Department also recognized in that decision that the object of the FCC's rules is "to achieve broad public access to competitive telecommunications services as quickly as possible through physical collocation." *Id.* at 12. By establishing service intervals for the provision of physical collocation space in that order, the Department "buil[t] upon the FCC's standards to provide greater certainty to the collocation process." *Id.*

As Verizon freely admits, it has long harbored hostility toward the physical presence of CLECs in their central offices on the grounds that CLEC access "diminish[es] the level of network security." Exh. AL-VZ 1-11. This hostility has evidenced itself in past proceedings before the Department and in Verizon's repeated appeals of federal rules establishing physical collocation as a requirement of ILECs. *See, e.g.*, *Verizon Tel. Co.* v. *FCC*, 292 F.3d 903 (D.C. Cir. 2002); *GTE Service Corp.* v. *FCC*, 205 F.3d 416 (D.C. Cir. 2000); *UNE Rates Order*, D.T.E. 01-20 (July 11, 2002) at 427; *Teleport Petition*, D.T.E. 98-58 at 7-9.

Verizon's latest attempt to restrain the development came in the form of an appeal of the FCC's *Collocation Remand Order* to the D.C. Circuit Court of Appeals, where it argued that the Telecommunications Act of 1996 allowed physical collocation on ILEC premises only when an off-site location was infeasible. *See Verizon Tel. Co.* v. *FCC*, 292 F.3d 903, 909 (D.C. Cir. 2002). The D.C. Circuit rejected this argument out of hand and upheld the FCC's interpretation of the Act's collocation requirements, which requires the collocation of equipment when an inability to deploy that equipment would, as a practical, economic, or operational matter, preclude interconnection or access to UNEs. *See id.*

In the face of similar ILEC arguments seeking to limit physical collocation, the FCC and Department have consistently supported the expansion of physical collocation arrangements. Indeed, the FCC has explicitly prohibited ILECs from "unreasonably restrict[ing] the access of a new entrant to the new entrant's equipment" through the adoption of unreasonable security measures. *Advanced Services Order*, at ¶ 48. Moreover, the FCC has warned that an "the incumbent LEC may not impose discriminatory security requirements that result in increased collocation costs without the concomitant benefit of providing necessary protection of the incumbent LECs equipment." *Advanced Services Order*, at ¶ 47.

The Department should recognize Verizon's current proposal for what Verizon candidly admits it is: the same anti-competitive collocation arguments that it presented, and the FCC and Department rejected, in years past.

C. VERIZON'S PROPOSED COLLOCATION RULE CHANGES SHOULD NOT BE IMPLEMENTED BECAUSE THEY ARE NOT THE MOST COST-EFFECTIVE SECURITY MEASURES FOR ADDRESSING RISKS AND THEIR PROBABLE HARM, AS DETERMINED BY AN APPROPRIATE RISK ASSESSMENT.

1. Verizon's Proposals, Especially Those Requiring Virtual Collocation Only, Impose Significant Costs On CLECs Without Any Demonstrable Improvement To Security.

Verizon's virtual collocation proposal would impose draconian costs and disruptions on CLECs and severely undercut the pro-competitive goals of the Telecommunications Act of 1996, without producing any demonstrable security benefit; in fact, such a proposal may actually be harmful, by precluding CLEC resources from service restoration efforts. Tr. 2, at 451-52 (Fea). As explained in more detail below, the evidence of cost and damage to public policy is overwhelming and – apart from conclusory statements by Verizon witnesses who could offer no support – unrebutted. As also explained below, based on the evidence in this case, the security benefits that would allegedly be realized from adopting Verizon's proposal are non-existent because there is no evidence that the collocators were responsible for any problems identified by Verizon. Indeed, Verizon has no idea who is responsible for the security breaches in its central offices. Tr. 2, at 453-54 (Nurse).

a. The CLECs' Detailed Testimony Regarding The Competition-Affecting Problems of Virtual Collocation Is Unrebutted By Verizon.

Requiring virtual collocation in Verizon "critical" central offices would have enormous impacts on CLECs. In both pre-filed and oral testimony, AT&T witnesses described in detail the myriad ways in which such a proposal would undermine AT&T's ability to compete. Exh.

ATT-1 at 17-18; Tr. 2, at 441-452. It would effectively gut facilities-based competition of its major competitive attributes. The three key benefits of physical collocation, which would be lost if physical collocation were not permitted, were summarized in AT&T's Rebuttal Testimony:

> First, physical collocation allows AT&T to control its own network facilities, thereby allowing AT&T flexibility in choosing how to manage and maintain its physical plant within the collocation site. In addition, physical collocation minimizes the inherent delays associated with virtual collocation since it typically does not require a collocation application every time network growth and rearrangements are required. Finally, it eliminates potential conflicts that may arise when an ILEC and AT&T are simultaneously trying to install or restore service in the same place, as was the case at the Verizon Manhattan West Street Central Office after the September 11th terrorist attack.

Exh. ATT-1, at 17. In addition, there are a host of other advantages of physical collocation:

1. The ability to provide our customers with a higher quality of service;
2. Control of provisioning intervals and mean time to repair (MTTR);
3. The ability to reduce long lead times regarding pre-provisioning items such as space, power and cabling;
4. Eliminating the need to maintain equipment spares and cabinets at every ILEC virtual collocation;
5. Eliminating the need to pay for new ILEC technician training every time an already trained technician is moved to different assignment;
6. Eliminating collocation application delays and issues that arise as a result of application process;
7. Eliminating potential for billing errors associated with collocation applications.

Id.

Moreover, at the hearings, AT&T witnesses explained in greater detail why each of the above-listed reasons for choosing physical over virtual collocation are real concerns, and not just make-weight arguments for this case. Perhaps the most problematic of all consequences of a virtual collocation only policy is the elimination of an essential element of facilities-based

competition. Mr. Gorham explained how a virtual collocation requirement would eliminate one of the main ways that AT&T competes with Verizon:

> From a local perspective on the operations side, I think that would really limit and restrict one of our areas that we compete with Verizon, and that's in response, response time to provide service, install new service when it's needed, test and turn up new equipment, as well as, once it's tested and turned up, to maintain it.

Tr. 2, at 441. Mr. Nurse elaborated on this point when he described TCG's competitive strategy: "We don't need to be perfect, we just need to be one step ahead of Verizon." Tr. 2, at 445. Further, Mr. Nurse also explained that the need to rely on Verizon will be particularly bad for CLECs seeking to meet specific service obligations that have already been negotiated, and agreed to, with individual customers. Tr. 2, at 446-447. He explained that, under industry performance metrics currently contemplated for development,[1] Verizon's only service obligation to AT&T will be to meet *average* performance standards, over the course of a month. Yet, in many cases, AT&T has specific service obligations with respect to individual customers. He stated:

> On the service-level agreements, we can have performance assurances with our retail customers. Those assurances are premised on our ability to provide a faster mean time to repair them[.] It's quite a legal problem for the Commission if you take away our ability to provide that improved mean time to repair. What are you going to do with those customer contracts? Are you going to break those contracts and relieve us of that obligation? Are you going to give the customer a fresh look and tell him, "We're not going to let AT&T give you two-hour mean time to repair any more. You can leave now"? And where are they going to go? That would be a substantial penalty on us as well as harm to our customers.

Tr. 2, at 446-447.

[1] Metrics for such performance are at best a year away from development and implementation. No effort is underway to develop them in the NY Carrier Working Group. Tr. 2, at 459-60 (Nurse).

The consequences to competition of a virtual collocation only policy are numerous and pervasive. Mr. Gorham, for example, worried that AT&T would no longer be able to go immediately to its own cage to install new equipment. Instead, AT&T would be "subjected to a 76-day interval between the time that we requested new equipment to be installed to the time it actually was installed." Tr. 2, at 442. *See also* Tr. 2, at 447.[2] Indeed, the Department is already well aware of the problems associated with "intervals" and delay that AT&T has had when it must rely on Verizon for the provisioning of facilities, as the Department has devoted an entire investigation to that issue in D.T.E. 01-34. *See also* Exh. VZ-ATT 1-23.

Moving on to other competition-affecting problems associated with virtual collocation, AT&T would no longer be able to maintain its own equipment. Instead of being able to obtain economies of scale associated with a central storage of spares, AT&T would have to incur the additional expense of providing spares to Verizon at a multitude of locations. Tr. 2, at 442. *See also* Exh. VZ-ATT 1-24 ("need to maintain an extra spares kit at each such location for use by Verizon technicians"). In addition, AT&T would have to incur the additional expense of training Verizon technicians. Tr. 2, at 443. And because Verizon technicians will not work on AT&T equipment as regularly as AT&T technicians do, they will be less familiar with it and less able to repair the equipment as rapidly as AT&T technicians. Tr. 2, at 443. Mr. Gorham gave a concrete example of the problem AT&T faces in relying on Verizon technicians by pointing to AT&T's experience with Verizon in the Westborough central office. Exh VZ-ATT-1-24. Mr.

[2] Mr. Nurse stated: "We have to pay an augment fee to change and modify, rearrange our collocations. Those are tariffed. We've taken administrative notice of the tariff. They also have intervals which are relatively long. So that increases our costs and slows down our response." Tr. 2, at 447-48.

Nurse explained more generally the impact that would result from AT&T reliance on Verizon technicians:

> We've spent a lot of money in our virtual collocation training Verizon techs on multiplexers. We use Lucent and Verizon uses Fujitsu. So we have to train Verizon technicians, which is an expensive undertaking. If you go to the recent Verizon work stoppage, where they had the strike, the Verizon technicians are going to go out. They're going to have less experience on our equipment than theirs because they're bigger than we are. In a work stoppage it's going to be worse, because you're going to be dealing with the management working during the strike as opposed to the craft. So we're concerned that that's going to leave us with substantially less qualified, less experienced personnel attempting to repair our equipment, even if they were willing to do it at parity in good faith.

Tr. 2, at 447. *See also* Tr. 2, at 496-497.

Moreover, it is not just the AT&T equipment that is unfamiliar to Verizon technicians. Verizon technicians will be unfamiliar with the way that AT&T has configured its physical collocation arrangement. The consequence of this is significant given Verizon's proposal for a new rule that requires virtual only where physical collocation arrangements currently exist. Only two alternatives exist for eliminating physical collocation arrangements, neither of which is satisfactory. If the physical collocation arrangements are converted "in-place" to virtual, Verizon would have to become familiar with what will seem like an "oddball" configuration. Tr. 2, at 448. This raises the same problems associated with Verizon technicians working on unfamiliar equipment. Alternatively, the physical collocation arrangement would need to be dismantled and reconfigured as virtual. *Id*. Although the exact cost and disruption of the second alternative has not been investigated or established in this record (because Verizon has not identified any specific central office for which virtual collocation would be required), the magnitude of such costs and disruptions are apparent.

Finally, it is overwhelmingly obvious from the record in this case that virtual collocation is simply unacceptable as a means of obtaining interconnection with Verizon. That is the

unanimous opinion of all users of virtual collocation. Sprint simply states that it "is unwilling to assume the business risk . . . of accepting virtual collocation from Verizon, and therefore has no actual experience in Verizon's virtual collocation." Exh. VZ-Sprint 1-11. Mr. Lathrop details WorldCom's problems with collocation at pages 9 to 11 of his testimony. Exh. WCOM 1. Covad's list of problems with virtual collocation are set out in its testimony on pages 7-10. Exh. Covad-1. Qwest objects to the whole notion that it is appropriate to exclude CLEC personnel from central offices. Exh. Q-1, at 11-12. Allegiance explains how it would be adversely affected by a requirement that physical collocation arrangements be converted to virtual on pages 8-10 of its testimony. Exh. AL-1. Moreover, the Department does not need to rely on just what the CLECs *say*. The Department can look to what the CLECs *do*. Out of 781 total collocation arrangements in Massachusetts, only five are virtual. Sprint Exhibit 1, at 7 (referencing information request Conversent 1-1a, attached thereto).

Nowhere in the record of this case does Verizon attempt to respond to the overwhelming and detailed evidence regarding the adverse impact of requiring virtual collocation. Indeed, Verizon does not even attempt to address with specificity a single one of the problems related to virtual collocation that the CLECs have raised, with two exceptions that are easily dismissed. First, Verizon takes issue with Covad's claim that Covad will have to wait the full length of an equipment installation interval when Covad wants to introduce a new service. According to Verizon, if a new service does not require an equipment installation, then Covad would not have to wait. Exh. VZ MA 2, at 16-17. This is shameless obfuscation. Verizon seeks to draw attention from the truth, which it ignores: if a new service does require an equipment installation, then Covad would have to wait. Likewise, Covad would have to wait for a

reconfiguration of this existing equipment. Even loading software may be subject to delay and associated fees. The result is delay of service to Covad's customers and higher costs for Covad.

The only other counterargument that Verizon offers regarding virtual collocation relates to the expense of training Verizon personnel. In this case, Verizon's counterargument does not even address the WorldCom evidence that Verizon purports to rebut. WorldCom had testified that it is required to train Verizon personnel on WorldCom equipment and, indeed, had been required to hire a certified vendor to "translate" WorldCom engineering instructions into the Verizon format. Exh. WCOM-1, at 10-11. In response, Verizon *admits* that the CLEC is responsible for the initial training, adding only that the CLEC would not be responsible for retraining. Exh. VZ-MA 2, at 17. Moreover, Verizon's reassurance that no additional training is required where Verizon is already familiar with the equipment is cold-comfort to CLECs, like AT&T, which use different equipment from Verizon. Tr. 2, at 447.[3]

Instead of responding to the specific problems with virtual collocation that the CLECs identified, Verizon offered in response only conclusory statements to the effect that all the CLEC complaints cannot possibly be true, or if they are, they are "de minimus." Tr.1, at 50 (Shepherd). Yet, Verizon's witnesses readily admitted that they had done no analysis from which they could reach any conclusions regarding the impact of virtual collocation on CLEC operations. Tr. 1, at 46-49. Indeed, as noted above, Verizon had not even consulted with CLECs regarding the possible impact of its virtual collocation only policy on CLEC operations. Tr. 1, at 46. In light of Verizon's cavalier attitude toward CLEC concerns regarding a virtual collocation only policy

[3] Verizon's lack of experience on CLEC equipment makes matters even worse. After CLECs have incurred the expense of training Verizon technicians, they often find themselves called upon either to do the work or to closely supervise the attempts of inexperienced Verizon technicians to do the work. Exh. VZ-ATT 1-24.

evidenced in the record of this case, CLECs can be forgiven for dismissing Verizon witness Mattera's after-the-fact offer "to work with the CLEC community to minimize [virtual collocation] impacts" as self-serving, if not downright cynical. Tr. 50, at 16-19.

In summary, the record contains unusually detailed evidence regarding the detrimental effect of a virtual collocation policy on facilities-based competition. The record is devoid of any substantive response undercutting that evidence. Accordingly, a request by Verizon for the Department to find that the impact of prohibiting physical collocation would be *de minimus* would be tantamount to a request that the Department violate the substantial evidence rule. *Cohen v. Board of Registration in Pharmacy*, 350 Mass. 246, 253 (1966) (even if there is some evidence in the record from which a rational mind might draw the desired inference, under the substantial evidence rule, an administrative agency's decision cannot be contrary to the overwhelming weight of the evidence).

b. Verizon Presented No Evidence That Excluding CLEC Personnel From Central Offices Will Have A Positive Security Benefit.

The sole justification offered by Verizon for its proposal to establish virtual collocation only central offices is the simplistic claim that "reducing foot traffic" will reduce the likelihood of a security problem. *See, e.g.*, Tr. 1, at 63, 115; Exh. Sprint-VZ 2-4. Yet, nowhere in the record of this case has Verizon presented any evidence that the representatives of CLECs present a security risk.[4] Verizon simply claims that it is "logical" that the risk to the network increases with the number of non-Verizon employees present. Exh. Sprint-VZ 2-4. (Verizon nowhere explains why this is "logical," since Verizon cannot prove that its employees are not the

[4] Indeed, Verizon readily admits that it has prepared no analyses and has no documents showing that implementation of any of its proposal would have any security benefit. Exh. Sprint-VZ-2-6.

perpetrators of the security breaches against CLEC equipment.) Perhaps, however, Verizon would have reached a different conclusion had it actually analyzed the data it presented in this case.[5] The only risks that Verizon identifies are those that are reflected in the collocation-related, so-called "security breach" incidents that Verizon listed in Exh. AG-VZ 1-1. Not a single one of those incidents resulted in a reportable network outage and, more importantly, there is no evidence that a CLEC representative was responsible for a single one of the incidents in Massachusetts, as demonstrated by a listing of those incidents that occurred in Massachusetts. RR-DTE-2(b).[6] Indeed, in many of these cases, it is the CLEC that is the "victim" of the "security breach." AG-VZ 1-1. Moreover, when the listed network outages are analyzed, it turns out that, in six of the seven outages in the record, the cause is a Verizon employee, and in no instance is it a CLEC employee. RR-DTE-VZ-3. (The seventh outage was caused by a water company.) Given the foregoing evidence, it is hard to understand how excluding CLEC employees from Verizon central offices will improve security and reduce the risk of network outages.

Perhaps most troubling of all about Verizon's "foot-traffic reduction" argument is the discriminatory implementation of it. Why has Verizon singled out only its competitors for exclusion from central offices? Although it is "considering" other possibilities, it has no current plans to reduce foot traffic arising from any source other than CLECs. Tr. 1, 140, lines 6-10; *See*

---

[5] The only data in the record of this case are data that have been requested by the Department and the parties. It is not data that Verizon has systematically developed as part of a properly performed risk assessment. Nevertheless, given Verizon's failure to develop an appropriate risk analysis, it is all that is currently in the record.

[6] Clearly Verizon had not looked at its own data when it stated that "[t]he types of security breaches that may be minimized or prevented by adopting Verizon MA's collocation security proposal are included, but not limited to, those violations described in Verizon MA's Reply to AG-VZ 1-1." Exh. Sprint-VZ 2-5. Verizon's own data fails to identify a single incident that would have been prevented by the exclusion of CLECs from Verizon central offices. RR-DTE-VZ-2(b).

also Tr. 2, at 338. Presently, Verizon permits a range of vendors, contractors, cleaning crews, and Verizon employees with no central office network responsibilities to enter the central offices Exh. AL-VZ 3-1.[7] Yet, it has made no proposal to exclude any of them.[8] Given the absence of any evidence that Verizon's competitors were the cause of a single security problem, Verizon's "foot traffic reduction" justification for excluding Verizon's competitors and no one else rings hollow indeed. In fact, given the fact that it is Verizon's competitors who are often the victims of the "security breaches" identified by Verizon, Verizon's proposal appears to be a classic example of a "blame-the-victim" solution to the problem. Tr. 2, at 453, line 18, through 454, line 16 (Nurse).

2. If Verizon Were Serious About Its "Concerns," There Are Other Measures That Verizon Could Implement That Would Address Those Concerns More Cost-Effectively.

If Verizon had really wanted to solve its problems, it would have proposed cost-effective measures targeted to the specific problem identified, not broad, sweeping proposals that inflict "collateral damage" principally on its competitors. For example, Verizon identified risks to

---

[7] Verizon claims that it does not permit Verizon employees who do not have central office responsibilities into areas of Verizon equipment "with their muddy boots." Tr. 1, at 223 (Mattera). It does, however, permit those employees into common areas for use of such facilities as restrooms. Tr. 1, at 224-25 (Reney). If it is necessary to exclude CLEC employees from the central office building altogether even though (a) the CLEC has equipment in the building and (b) has no access to Verizon's equipment (Tr. 1, at 164, lines 7-20), then why is it acceptable to permit Verizon employees into the building when they have absolutely no business or professional reason for being there? According to Verizon, the mere presence of someone in the building, even though he/she doesn't have access to Verizon's equipment, is a security risk. If Verizon's goal were to reduce foot traffic in the building, and not to disadvantage competitors, then perhaps Verizon would have reduced access of non-essential Verizon employees. It should also be noted that, when pressed, Verizon was unable to support its argument that the mere presence of someone in the building presents a security risk. It turns out that the likelihood that someone in a building without access to Verizon equipment will present a security risk depends on the specific configuration of each central office. Tr. 1, at 164, lines 21-22. This is not surprising, since risk assessments must be performed on a site specific basis, and Verizon has not presented any such analysis.

[8] Verizon was evasive as to whether and how it would address the non-discrimination requirement in the FCC rules prohibiting Verizon from burdening CLECs with security measures that are more restrictive than those applicable to itself or its vendors. Tr. 2, at 339, line 2 (Craft).

"COs with . . . emergency 911 ("E911") switches and adjunct equipment . . . which is critical to the network as they are used to complete interoffice and emergency calls." Exh. VZ MA 1, at 26. It would, of course, be far more cost-effective to post guards at such facilities rather than to impose the disruption of excluding all other telecommunications carriers from the facilities.[9] Yet, Verizon insists that a far more costly and disruptive security measure, *i.e.*, the exclusion of CLECs altogether from such facilities, is warranted. If Verizon wants to implement any changes to security at its central offices, it should identify measures that could address in a targeted fashion the problems that this record discloses.

In fact, the security measures that Verizon claims to use already will address Verizon's concerns, if Verizon implements those measures properly. Exh. ATT-1, at 11-12. Verizon claims to currently use the following security measures: (1) non-Verizon employee collocation identification cards, (2) electronic card reader access systems, (3) key controlled access systems, (4) directional signage and floor markings (*e.g.*, floor tape), (5) access through guarded entries, and (6) security cameras (*i.e.*, Closed Circuit Television ("CCTV")) in COs with cageless collocation open environment ("CCOE"). Exh. VZ MA 1, at 17. Verizon then argues against a straw man by trying to explain why (only) two of the six measures *alone* do not provide sufficient security. *Id*., at 19-21. Verizon simply avoids answering the obvious question of why

[9] It should be noted that, at the same time that Verizon identifies E911 equipment as vulnerable to security risks, it admits that the E911 system has multiple levels of redundancy built into it. Exh. VZ MA 2, at 15. There is no single point of failure. *Id*. There are four E911 control tandems in Massachusetts. *Id*. As a result, at least two would have to become disabled at the same time in order for certain areas to lose E911 service. *See, e.g.*, Attachment to RR-DTE-VZ-3. (VZ reroutes traffic from incapacitated E911 tandem to a working tandem). Even in that case, however, traditional 911 service would not be lost. Under basic 911 service, 911 calls are routed to the designated public safety agency such as the police department primarily associated with the central office. (Obviously where a larger town and a smaller suburb have a common CO, under basic 911 the emergency call is typically routed to the larger town's public safety point, but this was the arrangement for decades and remains today in some locales, outside of Massachusetts.)

its security measures *in combination* are not adequate. In fact, as AT&T explains, they will work well if properly implemented. Exh. ATT-1, at 12.

In its panel testimony, AT&T reveals Verizon's claimed reasons for why Verizon's current security measures are not adequate as the straw men that they are. Exh. ATT-1, at 12-16. As AT&T's witnesses state, "the reasons that Verizon gives for the alleged inadequacies of its current measures are not reasons that any reasonable security expert would use for rejecting a security measure in favor of [a] far more expensive and impractical policy." Exh. ATT-1, at 13. AT&T witnesses take on each of Verizon's bogus arguments:

> The claim that current measures are not preventative is not accurate. Every measure that makes the undesirable behavior to which it is targeted less likely is preventative. Dummy cameras are often used to give people the impression that they are being watched. When access card readers with anti-passback features are used, it acts as a deterrent because individuals will know that their presence can be traced to the location and time when an incident occurs.
>
> The claim that cameras do not capture every angle and are not "real time" is not a reason to implement alternative, draconian measures. Cameras fitted with motion sensors, can, in fact, be set-up for real-time operation and viewing. Moreover, the ability of cameras to capture "every angle" is very much a function of how the cameras are positioned and how many cameras are deployed. The choice between adding a few more cameras, on the one hand, and implementing costly and impractical collocation rules on the other should be driven by an evaluation of costs and benefits.
>
> The claim that access cards only provide a witness or suspect after the fact and do not show when an individual leaves is not accurate. As mentioned earlier, access cards can be an effective deterrent. Moreover, access systems come with various options. While some require swiping on entrance only, others require card swiping on entrance and exit. This is a feature know as "anti-passback". Some allow activation for certain periods of time based on the individual card. There are also high technology biometric devices that require authentication based on fingerprints or retinal scans. On the low end of the scale are key and/or combination locks.
>
> Finally, the claim that breaches of security protocols by CLEC employees go unpunished because Verizon does not have the same recourse against

> CLEC violators as it does with its own employees or vendors does not make sense. Verizon certainly has the right to bar entry of any individual to its central offices by revoking an individual's access authorization. Indeed, Verizon's current rules permit it to bar offending CLEC personnel from central offices through the deactivation or recovery of access key cards.

Exh. ATT-1, at 13-16. *See also*, Tr. 2, at 484-485 (Verizon can deny access to CLEC employees guilty of security breaches). Each of these AT&T arguments are set forth in more detail in its panel testimony. Exh. ATT-1, at 13-16.

Perhaps the only thing lacking in Verizon's current security measures is proper analysis of the information Verizon gathers and proper communication with the CLECs whose facilities have been placed at risk by certain incidents. Mr. Paszynsky explained how AT&T would use the information that Verizon had collected:

> Well, we have a system that is similar in that security incidents across the AT&T enterprise are tracked in a database, and that's something that we've done since 1982. The use of the database, however, is much, much more than a collection tool, which I think is represented by the binders that were given to me, the Verizon incident reports. What we do is to analyze the data. We group it. We look for trends. And if the shoe was on the other foot here in this instance, the very logical thing to do here would have been to provide -- to generate some ad hoc reports and to look at which of these collocation facilities is generating the more significant incidents, pick up the phone, call someone at AT&T, preferably in a corporate-security environment, make AT&T aware of this, and ask for some help in some sort of correction. Raw data, which this is, is of absolutely no value. It has to be massaged. It has to be culled, it has to be looked at, and it has to be acted upon. I would present to Madam Hearing Officer that this is what we currently do, this is what we have done for a number of years in my organization. We've actually taken a very proactive stance, and obviously, this is what you need to do to prevent problems from recurring.
>
> *********
>
> And I guess also, one would wonder how many of these binders of incident reports would have to be collected before they become such a problem that they eventually are reported to AT&T. Is it three? Is it four? Is the magic number double what we presently have over a period of two years and some-odd months? *Just why, why were these incidents, if they*

were so egregious to Verizon, not brought to the attention of the organization that could have aided in getting them resolved?

Tr. 2, at 452-454 (emphasis added). *See also* Tr. 2, at 440, lines 17-21. As illustrated by AT&T's approach, the obvious steps that Verizon should have taken, but did not, raise questions about Verizon's real concerns and motivations in this case.

In summary, if Verizon had conducted a proper analysis and communicated with CLECs regarding its findings, Verizon could have addressed any legitimate security concerns its analysis revealed in a cost-effective manner. Moreover, it is likely that the result of such an analysis would meet with the approval of CLECs whose equipment is at risk from Verizon's failure to implement those cost-effective measures.

III. VERIZON'S PROPOSAL CANNOT BE IMPLEMENTED.

A. VERIZON'S PROPOSED COLLOCATION RULE CHANGES VIOLATE THE TELECOMMUNICATIONS ACT OF 1996.

The plain language of the Telecommunications Act of 1996 ("Act") requires that Verizon provide CLECs an opportunity to physically collocate within Massachusetts central offices. Specifically, section 251(c)(6) requires ILECs to "provide on rates, terms, and conditions that are just, reasonable, and nondiscriminatory, for physical collocation of equipment necessary for interconnection or access to unbundled network elements at the premises of the local exchange carrier." 47 U.S.C. § 251(c)(6). The language of section 251(c)(6) has been repeatedly interpreted as establishing a *requirement* upon the ILEC to provide CLECs with physical collocation space. *See, e.g., Verizon Tel. Co.* v. *FCC*, 292 F.3d 903. The statute provides for only two exceptions to this requirement, when an ILEC can demonstrate to a state commission that "physical collocation is not practical for technical reasons or because of space limitations." 47 U.S.C. § 251(c)(6). These remain the only two exceptions to the federal physical collocation requirement, as the FCC has not expanded upon these exceptions within its regulations, 47

C.F.R. 51.323(l), nor does it have the authority to do so. *See Martinez* v. *Rhode Island Housing & Mortg. Fin. Corp.*, 738 F.2d 21, 26 (1st Cir. 1984) (an agency rule out of harmony with the authorizing statute is a "mere nullity", citing to *Manhattan Gen. Equip. Co.* v. *Commissioner*, 297 U.S. 129, 134 (1936)).

Verizon's proposal, particularly its recommendation that certain central offices be classified as critical "virtual collocation only" sites, is in direct conflict with the physical collocation requirements established under the Act. Verizon's proposal would eliminate physical collocation altogether at these critical sites. This problem is exacerbated by the vague nature of Verizon's criteria for determining what central offices should be deemed critical. Exh. VZ MA-2, at 15, lines 1-11. Verizon has stated that central offices that service military installations, airports, major businesses and public agencies would be potential "virtual only" sites. *Id.* Such broad criteria could potentially lead to the widespread disappearance of physical collocation throughout Massachusetts. Indeed, Verizon's hearing witnesses were unable to provide any hard number regarding how many central offices would fit within this criteria. Tr. 1, at 83-84 (Reney, Shepherd). Clearly, the clear language of the Act prohibits such a result. 47 U.S.C. § 251(c)(6) As the FCC has recognized, "driv[ing] competitors to opt for virtual collocation even though physical collocation is technically feasible, frustrat[es] the 1996 Act's preference for physical collocation." *Collocation Remand Order* at ¶ 93.

Moreover, the Department does not have the authority to adopt such a proposal. While the federal statute expressly encourages state commissions to establish requirements that further the purpose of the Act, it does not grant the Department authority to adopt proposals that conflict with federal requirements. 47 U.S.C. § 261(c) requires that state regulatory bodies adopt requirements "not inconsistent" with the requirements of the Act.

When it becomes impossible for a carrier to comply with the directives of the Department and the requirements of the Act simultaneously, state and federal requirements are in conflict and the Department's action is preempted. *E.g., Arthur D. Little, Inc.* v. *Comm'r of Health and Hospitals of Cambridge*, 395 Mass. 535, 550 (1985). Once ordered by the Department to establish certain virtual collocation only sites, Verizon would be unable to continue to comply with the federal requirements concerning physical collocation. Thus, federal and state requirements would conflict, and the Department's action would be preempted. Likewise, the federal statute's physical collocation requirement would also preempt any Department action making the transfer of unsecured CCOE arrangements to virtual collocation mandatory.

Indeed, Verizon concedes that much of its proposal is inconsistent with federal requirements by suggesting that the Department would be able to seek a waiver of those requirements from the FCC. Despite Verizon's allusions to the contrary, the Department could not avoid preemption by seeking such a waiver. Exh. VZ MA-2, at 27, lines 15-18. The statute's requirements were established by Congress, and neither the FCC or Department have the authority to waive those requirements. *See Martinez*, 738 F.2d at 26.

Verizon makes another attempt to clear the hurdles established by the Act by making the wholly unsupported claim that its security proposal is a response to the "technical feasibility" concerns of the Act. Exh. VZ MA-2, at 27, lines 1-2. This half-hearted attempt to fit drastic measures such as virtual collocation only central offices within the technical practicality exception to the Act's physical collocation requirement should be ignored by the Department. Verizon has made no showing whatsoever that security concerns raised in this proceeding rise to the level of making physical collocation technically impractical. Indeed, as outlined in Section IV below, there are a number of simple uses of currently available technology that are more than

adequate answers to whatever Verizon's security concerns are. Verizon's contention is thus meritless.

B. VERIZON'S PROPOSED COLLOCATION RULE CHANGES VIOLATE FCC ORDERS THAT, CONTRARY TO VERIZON'S CLAIMS, REMAIN VALID AFTER SEPTEMBER 11TH.

Verizon's proposals also violate several FCC regulatory orders that continue to govern the provision of collocation arrangements, despite Verizon's contentions to the contrary. Most notably, the FCC's *First Local Competition Order*, *Advanced Services Order* and *Collocation Remand Order* all confirm that the Act requires ILECs to make physical collocation at their premises available to CLECs. *First Local Competition Order*, ¶543; *Advanced Services Order*, ¶25; *Collocation Remand Order*, ¶85. This interpretation was recently affirmed by the D.C. Circuit Court of Appeals in *Verizon Tel. Co.*, a decision rendered after the terrorist attacks of September 11. *See* 292 F.3d at 905. In addition to the D.C. Circuit decision, the FCC has continued to apply the requirements of these orders to the provision of collocation services in the wake of September 11th. *See Virginia Non-Price Arbitration Order* at ¶531. Verizon's contention that September 11th has created uncertainty concerning the validity of these orders is thus baseless. Exh. VZ MA-1, at 15-16.

While most of the FCC's directives concerning collocation were released prior to September 11th, potential terrorist activity was certainly among the considerations taken into account by the FCC. The massive attack upon the Murrah Federal Building in Oklahoma City, after all, occurred in 1994, long before many of the FCC's orders. Clearly, the FCC can be assumed to have been aware of the loss of life in Oklahoma City when it subsequently issued its many collocation orders. The potential for major terrorist attacks is not something ignored by or unforseeable in the dilation of previous decisions concerning collocation policy. Verizon's insinuation that past orders did not cope with terrorism threats, therefore is unfounded.

C. VERIZON'S PROPOSAL IS TOO VAGUE TO IMPLEMENT.

In addition to the illegality of Verizon's proposal, large portions of it are too vague for the Department to implement. Verizon's proposal to restrict collocation at certain critical central offices to "virtual only," for instance, is so vague that it is difficult to discern what is being proposed. Verizon states that it will "work with the Department to assist the Department in determining which specific COs are critical." Exh. VZ MA-2, at 16, lines 19-21. When questioned as to what the Department would be approving if this proposal were accepted, Verizon's witness stated that the Department would be approving a "process." Tr. 1, at 84 (Shepherd). Presumably, once approved, additional hearings and testimony would be necessary for the Department to determine what central offices should be classified as critical sites.

Yet, Verizon has not even proposed clear criteria for this determination. As alluded to above, Verizon has set forth a variety of overbroad "factors important in assessing whether a central office is critical." Exh. VZ MA-2, at 15, line 12. These factors have included whether the central office serves major businesses, government entities, airports or emergency services. Exh. VZ MA-2, at 14-16. Verizon has chosen not to set out any firm statement of what criteria should be applied, however, preferring to wait for subsequent proceedings in which criteria would be selected with the assistance of the Department. Clearly, Verizon is hoping that by winning a preliminary battle on "process" and avoiding specifics, it will eventually be able to push through a measure that will have extreme anti-competitive effects in Massachusetts. The Department should ignore such machinations and see Verizon's proposal for what it is – an opportunistic attempt to turn back the clock and restrict physical collocation at sites critical to CLEC's bottom lines.

Even if the Department took Verizon's proposal seriously, however, it would be impossible to implement. This proceeding was not commenced in order for Verizon to suggest a

"process" to the Department. The Department has chosen this proceeding – this "process" to resolve collocation security issues. Verizon's "virtual only" proposal does not provide the Department with a clear method to resolve potential security concerns and it should be rejected due to its vagueness.

IV. IF THE DEPARTMENT FINDS IT NECESSARY TO ORDER IMPLEMENTATION OF ADDITIONAL SECURITY, THE DEPARTMENT SHOULD IMPLEMENT ONLY THOSE MEASURES SUPPORTED BY THE EVIDENCE IN THIS PROCEEDING.

As noted elsewhere in this brief, the security concerns that Verizon identified in this case are not new concerns. They are the types of concerns that ILECs have raised for years regarding collocation issues. As identified by Verizon, those concerns involve such things as unauthorized entry into central offices, theft, vandalism, drug use and other improper conduct of that nature. Exh. VZ MA 1, at 21-12; Exh. AG 1-1. Because these issue were well understood at the time that the present collocation rules were established, there is no need to change those rules now. Nevertheless, the Department may wish to consider requiring Verizon to take certain steps, that do not necessarily involve collocation rule changes, to protect the public switched network, especially – given the evidence in this case – the parts of the network owned by CLECs. In general, the steps recommended here are the types of procedures and policies that Qwest, in its capacity as an incumbent in its home territory already employs. *See generally*, Tr. 2, at 591-598 (Andragna); Exh. Q-1, at 19-23.

In particular, given the evidence in this case, it would be appropriate for the Department to require Verizon to improve its method for recording and analyzing "security" violations, improve its method for communicating with CLECs regarding security issues, upgrade its screening protocols to require more frequent background checks on all persons with access to

Verizon central offices, including existing Verizon employees and vendors, and deploy a CRAS system with an anti-passback feature, as discussed in greater detail below.

A. IMPROVEMENTS TO VERIZON'S METHOD FOR RECORDING AND ANALYZING "SECURITY" VIOLATIONS.

It is clear from the record in this case that Verizon has an inadequate system for recording security violations and absolutely no system for analyzing and acting on the information that it records. Reports of incidents are received and recorded in two different organizations (Ms. Reney's collocation group and Mr. Jacobs' security organization), with poor coordination between them. Tr. 2, at 386, lines 19-20. Importantly, the person in Ms. Reney's organization responsible for recording the incident is a clerk-level employee with no experience or training in determining whether an incident is a security violation or not. As a result, many incidents are coded as "security breaches" when they are not. Tr. 2, at 455-456 (*e.g.*, plugging a transformer of the sort that is on a cell phone into a convenience outlet). *See also* Tr. 2, at 464, lines 7-9.

Moreover, it is also clear from the record in this case that Verizon has little experience with analyzing the data collected. When Verizon reported the data in response to the information request AG-VZ 1-1, there were many duplications. It was evident that Verizon security analysts had never tried to look at the data: the duplications had to be removed by hand in response to a record request from the Department in this case. RR-DTE-VZ 2(c). Moreover, Verizon was unable to sort its data by state, much less by central office. Such an ability is essential to proper analysis. Mr. Paszynksy gave an example of how AT&T analyzes its data:

> Well, that was driven by the fact that years ago we were seeing repetitive instances of the same types of investigations, such as, let's say, laptop thefts. Obviously, you know, you don't want to wait around for the next and the next and the next. You want to get to the heart of the problem. So what you do is, you develop an action plan with the involved business unit, with prescribed dates for completion that will get you to your goal. Obviously, it's based on an audit philosophy. It uses audit characteristics,

> mapping out what a problem might be, and then applying the fixes as needed.

Tr. 2, at 469, lines 6-18.

Accordingly, it is necessary for Verizon to improve its method for recording and analyzing security violations before any other steps are taken to improve security.

B. IMPROVEMENTS TO VERIZON'S METHOD FOR COMMUNICATING WITH CLECS REGARDING SECURITY MATTERS.

It also became apparent in the proceedings that Verizon needs to improve its method for communication with CLECs regarding security matters. Despite the voluminous binders of so-called "security" incidents that Verizon produced in response to AG-VZ 1-1, Verizon contacted AT&T on only one occasion relating to a rather trivial matter of trash in a collocation cage. Tr. 2, at 455. Yet, on security matters that warranted communication between AT&T and Verizon, Verizon remained silent. It was AT&T that had to contact Verizon. Tr. 1, at 76-77. Indeed, Mr. Jacobs, whose responsibility is "to liaison" with a CLEC affected by a security problem, did not even seem to know who the AT&T person is with whom he is "to liaison." Tr. 1, at 76-77.

As a general matter, Verizon notifies CLECs regarding security matters by posting its Collocation Security Guidelines on its web site and expecting CLECs to check those guidelines from time to time. Tr. 1, at 105-106. Verizon also sends out mass distribution e-mails with "industry letters" to CLECs relating to any and all matters that may affect them. Tr. 2, at 616, at line 5 (Cullather). Apparently, among the constant flow of industry letters are some that relate to security matters. Tr. 2, at 615 (Cullather). Yet, there is no effective means to filter out security matters from the continual stream of industry reports.

Verizon's system of communicating general matters and its system of informing CLECs about specific events are not adequate. In both instances, there should be a single point of contact.[10] Especially given the recent financial problems of the telecommunications industry, and the concomitant downsizing of CLEC staffs for monitoring the countless industry rule changes that issue from ILECs almost daily, there should be a much more targeted line of communication regarding changes in security procedures. Verizon's distribution list for e-mails regarding security should not be the same list that it uses for the countless other notices that issue constantly. Moreover, the subject matter line of the e-mail should clearly indicate that it is related to security. Finally, the Verizon person responsible for security in Massachusetts should know the name and telephone number of the contact person at each CLEC collocated anywhere in Massachusetts.

C. MORE FREQUENT BACKGROUND CHECKS.

One of the most effective means of improving security is proper background screening of individuals with access to central offices. Tr. 1, at 94-95.[11] As a result, Verizon is implementing more stringent background checks for new hires. Tr. 1, at 95-96. For example, Verizon is changing its procedures to require a check of a potential hire's prior seven years, an increase of two years over prior requirements. Tr. 1, at 95-96. Despite the effectiveness of background screening, Verizon currently grandfathers all existing employees, both Verizon and CLEC, from

---

[10] Verizon already has a single point of contact for ID badges. Tr. 2, at 598 (Cullather). It does not, however, have a single point of contact for security measures as recommended here.

[11] Mr. Craft testified that that "knowledge about the characteristics and the integrity of the people with access to [central office] space is an important aspect of security." Tr. 1, at 94-95. Later, Mr. Craft apparently realized that such a statement is inconsistent with Verizon's unwillingness to apply background screening to current employees and tried to change his testimony, denying that he had stated that a person's background is a good indicator of potential future activity and claiming instead that a person's background is only a "possible indicator" of potential future activity. Tr. 1, at 201-202.

background checks, even if that employee has not been subject to a check for twenty years. Tr. 1, at 97-98. Such a policy disproportionately grandfathers Verizon's employees.

There is little doubt that Verizon's grandfathering provisions undermine security at its central offices. Mr. Jacobs, who is responsible for Verizon central office security in Massachusetts, testified that the more recent the bad conduct is, the more relevant it is to evaluating security risk. Tr. 1, at 204 (criminal activity yesterday is more relevant than criminal activity five years ago). Indeed, Verizon's witnesses readily agreed that applying the new more stringent background checks to current employees has the potential to reveal information that is relevant to security and has the potential to improve security. Tr. 1, at 100-101. Yet, Verizon exempts current employees from background checks no matter how long they have been employees.

There are apparently other considerations that Verizon is weighing against improved security. Verizon, however, has been unwilling to reveal what those considerations are and how Verizon arrived at its conclusion that they outweigh an undisputed improvement in security. If the Department concludes as a result of this case that there is a risk to network security, elimination of Verizon's exemptions for background screening would be an effective means of addressing the security problem, provided that Verizon acts on the results of such background checks in a non-discriminatory fashion.

D. DEPLOYMENT OF CRAS SYSTEMS WITH ANTI-PASSBACK FEATURES.

At the same time that Verizon says that key access is unsatisfactory (Exh. VZ MA –2, at 23, lines 19-20), Verizon contends that it plans to expand the use of electronic card reader access systems. Tr. 2, at 283, lines 13-18; Exh. VZ MA-1, at 5, lines 6-8. Verizon's security witness, Mr. Craft, testified that CRAS "is a much better, much more effective way of controlling access and leaves an audit trail, versus the traditional lock and keys." Tr. 2, at 283, lines 18-20.

Verizon's plans, however, do not include the use of anti-passback features in the CRAS that it will deploy. Tr. 2, at 28, lines 8-12; Tr. 2, at 290, lines 3-6. Such a feature would prevent a person who left a central office without swiping out his/her access card from reentering that office, or any other office. Exh. ATT-1, at 14, lines 15-16. Every card reader system has that feature should the facilities operator choose to activate it. Tr. 2, at 284, lines 15-20. Because a person who fails to swipe out would not be allowed back in, there would be a strong incentive for all persons to swipe-out. This, in turn, would ensure the recording of information necessary to determine who is in the building at any particular time. The CRAS that Verizon now intends to deploy, which does not include the anti-passback feature, does not permit Verizon to determine who is in the building at any particular time. Tr. 2, at 360, lines 2-11. The anti-passback feature, therefore, significantly improves the "audit trail" characteristic that Mr. Craft believes is important from a security perspective.

Despite the advantage of an anti-passback feature, Verizon witnesses in the hearings went to great lengths to resist recommending its use. Tr. 2, at 284-288. Remarkably, the main reasons that the witnesses offered for not using that feature were precisely the reasons that Verizon ignored when it recommended a virtual collocation only policy instead: cost and business inconvenience.[12] For example, Verizon cites to the relatively insignificant cost of installing an additional panel as a reason not to use the anti-passback feature. Tr. 2, at 288, lines 18-23. Verizon also cites the business inconvenience associated with a technician who – while working on equipment in the central office – leaves the building to retrieve a tool in his truck and forgets

[12] Mr. Craft also offered make-weight arguments related to health and safety to support Verizon's resistance to the anti-passback feature, but the hearing officer readily saw through those lame excuses. Tr. 1, at 284-285.

to swipe out. The technician would not be able to reenter to complete his work. Exh. VZ MA-2, at 23, lines 10-12.[13]

It is hard to understand why these examples of cost and business inconvenience warrant rejection of an anti-passback feature, when the cost and business disruption caused by Verizon's "virtual collocation only" policy does not. Clearly, if the Department believes that additional security is required at Verizon central offices, one of the first places to begin is with an anti-passback feature in Verizon's CRAS. Moreover, CRAS with an anti-passback feature has the additional benefit of improving the data available for analysis.

Conclusion

The Department should reject Verizon's proposed changes to the rules governing collocation arrangements in Massachusetts, for all the reasons set forth above, including Verizon's failure to perform the very analyses recommended by its own experts. Because the risks identified in this proceeding involve risks to CLEC equipment with concomitant degradation of service quality to CLEC customers, and because Verizon has not implemented procedures and equipment necessary to protect CLEC equipment, the Department should order Verizon to do so, in accordance with AT&T's recommendations set forth above.

[13] Verizon witnesses also raised such make-weight arguments as the feature would not always be effective, especially where "tailgating" upon entry occurs. Tr. 2, 285-86 (Mattera). There are two problems with this excuse for not implementing an anti-passback feature. First, no system is 100% effective, so the fact that the anti-passback feature is not 100% effective is not a reason not to implement it. Second, cameras and turnstiles can be used to monitor entry and prevent tailgating. Tr. 2, at 291. Such easy solutions reveal Verizon's make-weight arguments for the excuses that they are.

Respectfully submitted,

AT&T COMMUNICATIONS OF NEW ENGLAND, INC.

_____

Jeffrey F. Jones, Esq
Kenneth W. Salinger, Esq.
Jay E. Gruber, Esq.
John T. Bennett, Esq.
Palmer & Dodge LLP
111 Huntington Avenue
Boston, MA 02199-7613
(617) 239-0449 (voice)
(617) 227-4420 (fax)

Philip S. Shapiro
AT&T Corp.
111 Washington Avenue, Suite 706
Albany, NY 12210-2213
(518) 463-3148 (voice)
(518) 463-5943 (fax)

August 9, 2002