**COMMONWEALTH OF MASSACHUSETTS**

**DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY**

| | | |
|---|---|---|
| Investigation by the Department of Telecommunications and Energy 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 |

# REPLY BRIEF OF WORLDCOM, INC.

Christopher J. McDonald
WorldCom, Inc.
200 Park Avenue, 6th Floor
New York, NY 10166
(212) 519 4164
Fax (212) 519 4569
Christopher.McDonald@wcom.com

Dated: August 23, 2002

**TABLE OF CONTENTS**

**COMMONWEALTH OF MASSACHUSETTS**

**DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY**

| | | |
|---|---|---|
| Investigation by the Department of Telecommunications and Energy 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 |

# REPLY BRIEF OF WORLDCOM, INC.

## I. Introduction

In its initial brief, WorldCom, Inc. ("WorldCom") established that there is no reasonable basis for the Department to alter its existing collocation policies in favor of the anticompetitive and discriminatory proposals put forth by Verizon. In this brief, WorldCom responds to the arguments raised by Verizon in its initial brief ("Verizon Br."). Because much of what Verizon argues was anticipated by WorldCom and is addressed in WorldCom's initial brief, WorldCom will not repeat here all the reasons why Verizon's proposal should be rejected. Rather, WorldCom will respond briefly to some of Verizon's arguments, organizing its responses generally to follow the structure of the seven subsections (labeled A through G) in the Argument section of Verizon's brief.

## II. Argument

### A. Limiting CLEC access to Verizon's central offices and remote terminals is not necessary to enhance security

In its brief, Verizon continues to lump together "intentional" and "unintentional" conduct in its attempt to rewrite the rules for collocation in Massachusetts. *See e.g.*, Verizon Br. at 1, 2, 5, 16, 24, 26. But the two categories of conduct absolutely must be dealt with separately,

and an assessment must be made with respect to each category to determine whether limiting CLEC access to Verizon's central offices and remote terminals will actually achieve the "enhanced security" Verizon promises.

Verizon cannot dispute that the "threat" to network security from a CLEC technician *unintentionally* causing some network-affecting event is precisely the same today as it was before the events of September 11, 2001. It is precisely the same today as when the FCC addressed collocation security issues in its *Advanced Services Order*[1], and it is precisely the same today as when the Department addressed collocation security in its *Phase I Order*, *Phase I Reconsideration Order* or its *Phase I-B Order* in docket D.T.E. 98-57. In other words, all the arguments concerning CLEC technicians inadvertently damaging incumbent LEC equipment during their visits to central offices were fully known to, and considered by, the relevant decision makers at the time the current rules were put in place. And as discussed in WorldCom's initial brief, Verizon has presented no evidence in this proceeding to justify a change to current collocation rules as a result of past *unintentional* network affecting conduct on the part of CLEC technicians. WorldCom Br. at 14.

Moreover, the reason for this investigation, in the wake of September 11, 2001, is the threat of conduct on the part of those who intend to disable or destroy the telecommunications infrastructure. *See Vote and Order to Open Investigation*, at 1 (January 24, 2002). Verizon's arguments on that score also fail to advance its goal of restricting, or denying altogether, CLEC access to their collocated equipment. There is *nothing* in the record to suggest that CLEC technicians are any more likely to engage in criminal or terrorist activities than

Verizon personnel who work in central offices. Indeed, the real threat is *not* from CLEC or Verizon technicians who are authorized to be on the premises to legitimately carry out their job functions in Verizon-owned facilities. The threat to the Commonwealth's telecommunications infrastructure (or at least the *one* threat of relevance to this investigation) is the possibility that a person *without authorization* and intent on destroying or disabling telecommunications equipment will gain access to a Verizon central office. As such, the security imperative that must be addressed above all others is ensuring that only authorized individuals gain access *to the central office building*.

Verizon apparently subscribes to the view that the presence of collocators in its central offices has somehow altered that imperative:

> the CO building structure itself (*i.e.*, the exterior walls and doors of the premises) ***was*** the primary security measure to keep unauthorized individuals out.
>
> With the advent of physical collocation, circumstances changed. The equipment of multiple carriers is now placed in Verizon MA's COs, and many more individuals are allowed access to Verizon MA's facilities. The greater influx of "foot traffic" dramatically increases the security risks to the network infrastructure and directly affects the type of security measures that can and must be imposed.

Verizon Br. at 17 (emphasis added; citation omitted). WorldCom submits that circumstances *have not* changed, or should not have changed, in that the exterior of a central office should *still*

---

[1] *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, First Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 98-147, 14 FCC Rcd 4761 (March 31, 1999) ("*Advanced Services Order*").

be the "primary security measure" for keeping unauthorized individuals out.[2] Verizon, however, believes that

> [p]reventing other carrier personnel, who have a legitimate need to access their collocation space and are properly authorized to do so, from accessing areas containing Verizon MA's equipment, where they have no legitimate reason to be, is a critical security concern.

Verizon Br. at 24 (citation omitted); *see also* Verizon Br. at 17 ("the presence of all types of physical collocation inherently compromises Verizon MA's ability to protect its network from *within* the CO") (emphasis in original; footnote omitted). While there is no doubt that Verizon does have an interest in protecting its equipment from harm, a little perspective is in order. First, while a legacy monopoly provider, Verizon does not have a monopoly on honest, dedicated, hardworking employees. CLEC technicians, like their counterparts employed by Verizon, are perfectly capable of traversing through space housing Verizon's equipment (*e.g.*, to visit a rest room on the premises) or working in space near or next to Verizon equipment (*e.g.*, to perform maintenance on a CLEC's collocated equipment) without accidentally or intentionally causing damage to Verizon's network.

Second, Verizon presented no evidence supporting the notion that CLECs are the exclusive employers of technicians with a propensity to breach Verizon's security protocols or engage in other acts of misconduct. Indeed, as WorldCom explained in its initial brief, Verizon avoided the production of documents that would have revealed the extent to which its own

---

[2] It needs to be emphasized that WorldCom's and other CLECs' historical practice of confiscating and destroying the Verizon ID cards of terminated employees (*see, e.g.*, Tr. 411 (Allegiance); 508-09 (WorldCom)) does not compromise this goal. By destroying the access card, the unauthorized individual (*i.e.*, the terminated CLEC employee) would no longer possess the means by which to gain access to Verizon's facilities. However, having been made aware of Verizon's preference for having the cards returned upon an employee's termination, WorldCom will follow this procedure in the future.

employees have engaged in intentional or unintentional conduct resulting in damage to Verizon's network. *See* WorldCom Br. at 12-13 (discussing Verizon's response to information request AG-VZ-1-1).

Third, to the extent a CLEC employee or a Verizon employee were inclined to vandalize or steal equipment, security measures far less onerous than what Verizon proposes should serve as an effective deterrent in most cases. Even Verizon agrees that security devices such as cameras, electronic card readers, or badges with computerized tracking systems can deter security breaches. Exh. VZ-1 (Verizon Panel Dir.) at 2. And as discussed below, Verizon is taking steps to enhance security. The impact of Verizon's ongoing program of enhancing its security measures should be assessed before embarking on any plan to change existing policies.

Finally, although WorldCom certainly does not condone vandalism or thievery, there is a world of difference between a domestic troublemaker and an international terrorist. While the world has its share of miscreants who break things or steal things when they think no one is looking, none of the companies in this litigation – no organization of any kind – wants to have those people in their ranks. To the extent they avoid detection in the hiring process, get a job and get caught doing something stupid, reckless or harmful, there are mechanisms in place to deal with these people, ranging from intra-company disciplinary procedures to criminal prosecution. What Verizon is doing is using the threat of terrorism as an excuse to secure its network from perceived CLEC troublemakers, and it is using perceived CLEC troublemakers as an excuse to adversely impact the ability of CLECs to effectively collocate and compete with Verizon.[3]

[3] With respect to "authorized" versus "unauthorized" access, it is perhaps less far fetched than it once might have been to contemplate the possibility that someone who *is* authorized to be on the premises is, in fact, a "mole"

Unless and until Verizon comes forth with clear and convincing empirical evidence that the presence of CLEC technicians on Verizon premises would result in significant adverse impact to Verizon's network – and represents a greater threat to network security than Verizon's own technicians – there is no basis on which to assert, as Verizon does, that the reduction or elimination of CLEC "foot traffic" will make any central office in which CLEC equipment is collocated safer than it is today.[4]

### B. Verizon's "incidence of security breaches" does not warrant a change in collocation rules

Verizon is affirmatively asking the Department not only to change its settled collocation policies, but to petition the FCC for a change in federal collocation rules.[5] Yet the only affirmative evidence Verizon chose to have the Department consider was a brief list of

---

or "sleeper" in the employ of Verizon or a CLEC. Notable recent examples of this phenomenon in government are the cases of Robert Hanssen, the 25-year veteran of the FBI arrested last year, or Aldrich Ames, a 31-year veteran of the CIA arrested in 1994, both of whom sold classified information to the Soviet and then the Russian governments. In connection with the harms sought to be prevented here, a mole would be a telecommunications company employee intent on sabotaging the telecommunications infrastructure, but who has not yet taken action in furtherance of that intent. Of course, all responsible corporations, WorldCom and Verizon included, interview job applicants and perform some level of background check and/or drug testing help assess whether the individual would be a suitable employee. Exh. WCOM-1 (Lathrop Reb.) at 13; Exh. VZ-1 (Verizon Panel Dir.) at 5. Assuming, however, that these steps did not ferret out such an individual, one cannot reasonably conclude that limiting or preventing CLEC access to central offices would increase security. If anything, the fact that the mobility of CLEC personnel in Verizon central offices is *already* circumscribed in most instances (*see, e.g.*, Tr. 33; Exh. VZ-2 (Verizon Panel Surreb.) at 7) suggests that any individual seeking to gain "authorized" access to do damage from the inside would try to obtain employment with the incumbent, or with one of its contractors or cleaning companies, rather than with a CLEC.

[4] *See Local Competition Order* at ¶203 ("with regard to network reliability and security, to justify a refusal to provide interconnection or access at a point requested by another carrier, incumbent LECs must prove to the state commission, with ***clear and convincing evidence, that specific and significant*** adverse impacts ***would result*** from the requested interconnection or access")(emphasis added).

[5] The Department was invited to "join with Verizon to ensure that additional security measures can be implemented, and seek appropriate changes to FCC rules, if necessary." Exh. VZ-1(Verizon Panel Dir.) at 16. In spite of Verizon's more recent claim that its proposal is "consistent with the letter and the spirit of the Telecommunications Act of 1996 … and the [FCC] decisions enforcing the Act" (Verizon Br. at 2), its recognition of the need to "seek appropriate changes" is tacit acknowledgement that its proposal violates the FCC's current rules.

infractions in its initial testimony, many of which (*e.g.*, "theft and vandalism of Verizon equipment in secured and unsecured areas of the CO"[6]) may well have been committed by Verizon's own employees given that the culprits were never apprehended.[7] Of the infractions included in Verizon's responses to discovery, even Verizon admitted that some should not be categorized as "security breaches" (Tr. 72 (Jacobs)), and none of the alleged breaches resulted in an Verizon customers losing service. *See* Tr. 585-86; RR-DTE-VZ-3.

Moreover, with respect to the security breaches alleged to have been committed by CLEC employees, there is no indication that Verizon has sought the aid of CLEC management in addressing those breaches. For instance, to the extent that any WorldCom employees were alleged to have been involved in any of the security violations included in Verizon's discovery responses, Verizon never notified WorldCom so that corrective action could be taken. Tr. 517. Likewise, the panel testifying for AT&T confirmed that AT&T had not been contacted by Verizon with respect to any security breaches alleged to have been committed by AT&T employees. Tr. 455-56.

Clearly, CLEC employees on Verizon property should be expected to adhere to all reasonable safety and security requirements. To the extent that they do not adhere to such requirements, CLEC management should be informed so that appropriate corrective or disciplinary action can be taken, as necessary. Having Verizon better communicate alleged

---

6 Exh. VZ-1 (Verizon Panel Dir.) at 22.

7 *See* RR-DTE-VZ-2. Most of the evidence involving alleged security breaches – including the evidence confirming that no CLEC technician caused a Verizon network outage, and that Verizon itself was responsible for several outages – was not affirmatively provided by Verizon in support of its case, but rather was the product of discovery. *See id.*; *see also* RR-DTE-VZ-3 (documenting network outages caused by Verizon employees).

breaches is a simple step that could go far in reducing the number of incidents allegedly attributable to CLECs.

### C. Verizon's proposal is not reasonable

Section C of Verizon's brief walks through each separate component of Verizon's proposal. WorldCom has already expressed elsewhere in this brief and in its initial brief the reasons why Verizon's proposal is illegal, discriminatory and anticompetitive. WorldCom will simply reiterate here that it is opposed to Verizon's proposal to the extent that it (i) limits or delays WorldCom's access to its collocated equipment, (ii) increases costs for collocators, (iii) decreases the amount of total future collocation space potentially available to WorldCom[8] or (iv) violates existing federal collocation rules.

WorldCom has also previously articulated why Verizon's core rationale for its proposal, *i.e.*, the false logic of its "foot traffic" argument, is baseless. *See* WorldCom Br. at 13-15. In its brief, Verizon raises other arguments in favor of its proposal to which WorldCom will now briefly respond.

Verizon states that "carrier personnel may have less incentive to exercise care with Verizon's or other collocated carriers' equipment, or may be less trained or less familiar with the CO environment, and less aware of the potential incidental harm to the various types of CO equipment." Verizon Br. at 27. There is no evidence in the record to support Verizon's baseless assertion that CLEC personnel are less capable of working effectively in a "CO environment." More importantly, however, Verizon's "incentive" argument is completely off-

[8] *E.g.*, if some other CLEC would have been willing to obtain an unsecured CCOE arrangement, but would now take up space in the "segregated" section of a central office, that carrier's presence could conceivably restrict or preclude WorldCom's ability to obtain a collocation space at the facility in the future.

base. Even facilities-based CLECs are largely dependent on Verizon's network to reach their own customers. And Verizon has far more customers than any other local carrier. Metcalfe's Law states that the value of a network increases exponentially in relation to the number of users. It is therefore *always* in the interests of a CLEC and its technicians to ensure that the incumbent's network is up and running, because the value of the CLEC's network is dependent on the CLEC's customers' ability to reach *all* other end users in the local market, most of whom are Verizon customers.

It cannot be said that Verizon or its technicians have the same interest. The "value" of Verizon's network would not suffer appreciably if the customers of one or more CLECs were affected by outages. And as a competitor for those same customers, one could argue that CLEC outages benefit Verizon to the extent that they cause CLEC customers to return to the incumbent's network. Verizon's "incentive" argument thus falls flat.

Verizon also makes the claim that "the additional security [of its proposal] will benefit carriers by enhancing the security and reliability of their networks" and that its proposed plan "would apply equally to all collocators, and would not impede competition in any way". Verizon Br. at 2. One could almost argue that Verizon's positioning of its proposal as a net benefit to carriers – offering to save them from the folly of their own employees – smacks of paternalism. But paternalism implies that the ruling party ostensibly has the best interests of those under its control in mind. Again, that cannot be said of Verizon. The FCC itself has recognized that incumbent LECs "have incentives to overstate security concerns so as to limit

physical collocation arrangements and discourage competition."[9] And while barring all collocators from access to their equipment in so-called "critical" central offices certainly would put all collocators in those offices on equal footing with each other, it ignores the fact that CLECs do not compete only against each other, they compete primarily *against Verizon.* Verizon's proposal would unquestionably "impede competition" because a key CLEC selling point that attracts customers away from the incumbent – more rapid and responsive service – would disappear. *See, e.g.*, Exh. WCOM-1 (Lathrop Reb.) at 9-10; Tr. 445-446.

### D. Verizon's enhancement of existing security procedures should sufficiently address existing security concerns

Without any prompting by the Department, Verizon has begun the process of "enhancing" its existing security procedures. For instance, Verizon expects to complete the deployment of card reader access systems in Massachusetts within the next 18 months. Verizon Br. at 46-47. Yet Verizon also wants the Department to reach the conclusion that these enhanced security measures will be ineffective at preventing CLEC-caused harm to its network. *See* Verizon Br. at 43.

The Department should not adopt Verizon's hasty conclusion. Instead, the Department should follow a two-pronged approach before weighing any changes to its existing collocation rules. First, the Department should satisfy itself that Verizon is, in fact, enforcing its current policies. Verizon made the following observation in its brief with respect to the terrorist attacks of September 11th:

> it was not only crashing a plane, but the series of events leading up to that act (*e.g.*, lax enforcement of immigration policies, access to

[9] *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Fourth Report and Order, CC Docket No. 98-147, FCC 01-204, Released August 8, 2001.

> flight school lessons by those on 'high security watch' lists, failure to adequately screen airplane passengers for possession of weapons, etc.) that enabled the events of September 11th to occur.

Verizon Br. at 4, n. 4 (citation omitted). It would appear from that statement that Verizon agrees with the assessment of AT&T's security expert Michael Paszynsky, who testified that the overwhelming majority of security failures occur because the procedures "break down" and "are not followed" by the people to whom the security procedures relate. Tr. 462-63. Thus, before the Department contemplates any policy changes, Verizon should fully implement the safeguards it already has in place, as well as the ones it has promised, such as card entry systems.[10]

Second, the Department should allow sufficient time for Verizon's card reader and other enhancements to take effect before contemplating further action. Verizon obviously believes that its investment in additional security measures will pay dividends in the form of a more secure central office environment. The empirical evidence Verizon has provided to date does not warrant a change in state or federal collocation rules. A methodologically sound assessment of the impact and effectiveness of Verizon's enhanced security measures would certainly be in order before weighing something as radical as a change in state or federal collocation rules.

---

[10] However, in one critical respect Verizon's newly implemented guidelines concerning access cards and photo identification badges are discriminatory and anticompetitive. According to the July 2, 2002 CLEC Industry Letter attached to RR-ATT-2-2, a CLEC technician whose Verizon ID badge expires before it is renewed must go through a criminal background check and drug test. That is unfair, as it places an entirely unnecessary burden on CLECs and their employees. A person who continuously remains in the employ of a CLEC should be permitted to renew his or her Verizon ID badge, even an expired Verizon ID badge, *without* having to go through the process that a new hire goes through. Verizon has seen fit to "grandfather" these technicians anyway – there is no harm to Verizon if an otherwise authorized CLEC employee submits his or her renewal application for Verizon "access credentials" after previously issued "access credentials" have expired.

### E. There is no reason that other parties should have presented alternatives to Verizon's proposal

Verizon faults the CLEC parties for not suggesting alternatives to Verizon's proposal. But that can hardly be a surprise given that Verizon itself put forth a highly anticompetitive plan, and did so in the incumbent-versus-CLEC arena of an adjudicatory proceeding. Parties have naturally devoted the bulk of their energies toward the damage control function of seeing to it that Verizon's proposal is recognized by the Department as the anticompetitive ploy that it is. Moreover, there is no evidence to suggest that existing policies should change, so the fact that carriers did not suggest alternative policies is wholly unremarkable. Should the Department reject Verizon's proposal but decide to continue its investigation, WorldCom will continue to participate as the Department continues to pursue its goal of protecting the telecommunications infrastructure in Massachusetts.

### F. Virtual collocation is not a viable alternative to physical collocation

Verizon's section "F" is entitled "Virtual Collocation Is Recognized As A Viable Arrangement." WorldCom, and indeed the entire CLEC community, disagrees. This topic has been exhaustively covered by WorldCom and other parties. Verizon's assertions that virtual collocation is comparable to physical collocation is empty rhetoric in support of its attempt to disadvantage CLECs.

### G. What other carriers may require is irrelevant

Verizon seeks to justify its proposal by pointing to the security measures that other carriers require. Verizon Br. at 58. But such a comparison is inherently unfair, as it

wrongly assumes that Verizon's security measures must be inadequate if a CLEC does something more or different. It also assumes that Verizon is on the same competitive footing with CLECs. It is not. With the passage of the 1996 Act, it became the national policy of this country that telecommunications services – once the province of regulated monopolies – are subject to competition. That policy, as reflected in the Act and in FCC orders and federal regulations flowing from the Act, balances the legitimate security concerns of incumbent LECs with the legitimate requirements of competitive carriers to interconnect with the incumbent's network. Verizon may not like it, but CLECs having access to the former monopolists' premises is the law of the land.

## III. Conclusion

For all the foregoing reasons and for the reasons set forth in WorldCom's initial brief, WorldCom respectfully requests the Department to: (1) reject Verizon's proposals as both unnecessary and anticompetitive; (2) decline Verizon's invitation to change existing collocation policies in Massachusetts, and similarly decline to seek changes to the current collocation rules promulgated by the Federal Communications Commission pursuant to the Telecommunications Act of 1996, and; (3) monitor Verizon's ongoing efforts to bring its current security measures more up-to-date.

Respectfully submitted,

WORLDCOM, INC.

_____

Christopher J. McDonald
WorldCom, Inc.
200 Park Avenue, 6th Floor
New York, NY 10166
(212) 519 4164
Fax (212) 519 4569
Christopher.McDonald@wcom.com

Dated: New York, New York
August 23, 2002

**CERTIFICATE OF SERVICE**

I hereby certify that I have this day served the foregoing upon each person designated on the attached service list by email and either U.S. mail or overnight courier.

Dated: New York, New York
August 23, 2002

_____