Bruce P. Beausejour
Vice President and General Counsel – New England

185 Franklin Street, 13th Floor
Boston, MA 02110

Tel (617) 743-2445
Fax (617) 737-0648
bruce.p.beausejour@verizon.com

April 14, 2003

BY HAND DELIVERY

Mary L. Cottrell, Secretary
Department of Telecommunications and Energy
Commonwealth of Massachusetts
One South Station, 2nd Floor
Boston, MA 02110

Re: D.T.E. 03-38 -- Reply Comments of Verizon

Dear Secretary Cottrell:

Verizon Massachusetts ("Verizon MA") is filing this letter in reply to comments made by three CLECs – AT&T, WorldCom and NCI Telecom – in opposition to Verizon MA's request for a waiver due to the effect of the Slammer Worm. As discussed below, the arguments raised by the CLECs are without merit.

First, the CLECs claim that the Slammer Worm attack was not an "extraordinary" event beyond Verizon MA's control. Rather, they claim that the attack was a foreseeable event, which should not fall under the waiver provision of the PAP. The CLECs are wrong. While it is true that viruses and worm attacks occur frequently, what these CLECs fail to acknowledge is that Verizon has repelled other attacks, but the ferocity of this attack was much greater. This worm spread at extraordinary speed and affected many large businesses. *See* Petition at 6 ("the Slammer Worm open[ed] *a new era* of fast-spreading viruses on the Internet ...") (citation and quotations omitted); *see also* CNN.com./Technology "Looking into the mind of a virus writer," March 19, 2003 ("the malicious Slammer worm spread across the globe in 10 minutes ..."). The essential point glossed over by the CLECs is that while viruses and worm attacks may occur continuously, *see id*. ("[a]bout 1,000 viruses are created every month by virus writers..."), the Slammer Worm represented a new, much more dangerous breed.

Despite the continuous onslaught of viruses and worm attacks, this is the first time since the PAP was instituted for Verizon (beginning in New York in January of 2000) that a virus or worm has had any impact on Verizon's ability to provide services to CLECs. Moreover, the mere fact that viruses and worm attacks are foreseeable is not a rational basis on which to deny the Waiver Petition as these CLECs claim. In fact, as Verizon pointed out in its Petition, the

New York Public Service Commission ("NY PSC") granted a PAP waiver for a Work Stoppage in August 2000, though work stoppages are foreseeable. *See* Petition at 8-9 and note 7. In essence, the CLECs are arguing that Verizon should be held strictly liable when it has not been able to satisfy a PAP standard due to outside circumstances. The NY PSC rejected similar arguments when it approved the 2000 Work Stoppage Waiver.[1] The Department should reach the same result here.

Second, AT&T and Worldcom claim that Verizon MA is not entitled to a waiver because the Slammer Worm attacked a known vulnerability in Microsoft's SQL Server 2000, and that Microsoft had developed a patch for this problem months ago, which Microsoft had designated as a "critical" patch. WorldCom Comments at 2-3; AT&T Comments at 11-12. AT&T goes to great length to quote from various Microsoft bulletins regarding the application of security patches and states that the Department need only consider the practices of Microsoft in evaluating whether Verizon acted in a prudent manner. AT&T Comments at 10-11. Verizon MA agrees that Microsoft's experience is instructive. But it is Microsoft's actions, not its words, that are most informative – particularly Microsoft's inability to protect its own systems despite the availability of patches that it deemed to be critical. As is well known by now, the Slammer Worm attacked Microsoft's own systems and networks. Despite AT&T's contentions that patch management is a snap and that Verizon could have easily installed the necessary patch, industry observers have made it clear that "Microsoft's own actions show that you can't reasonably expect people to be able to keep up with patches." Petition at 11 (quotations and citations omitted). Penalizing Verizon for failing to fully install a particular patch – even a so-called "critical" one – that was not even fully installed by its maker would be patently unreasonable.[2] Indeed, in the aftermath of the Slammer worm, security experts suggested that such attacks are "inevitable" and that companies should "focus on limiting their damage, rather than expending every effort trying to create an ironclad perimeter." *Id.* at 12.

The CLECs trivialize and severely understate the time and effort required to test and apply the myriad patches released by software vendors in addition to other systems maintenance activities. Thousands of patches are announced annually by Verizon's software vendors. In 2002, Verizon applied over 27,000 software patches to Microsoft servers alone. Verizon's internal computing network contains over 233,000 addressable devices. As Microsoft acknowledged, the Slammer Worm required only ***one*** device without the appropriate patch to create the flood of network traffic across the internal computing network. *Id.* at 3 (citation and quotation omitted).

---

[1] Case 99-C-0949, et al., Petition of Bell Atlantic - New York for Approval of a Performance Assurance Plan and Change Control Assurance Plan, filed in C 97-C-0271, "Order Granting in Part and Denying in Part Requests for Waivers of Service Quality Targets" (issued June 7, 2001), at 4-5.

[2] Moreover, the "critical" designation is hardly the red alert that the CLECs make it out to be. The CLECs fail to mention that Microsoft designated as "critical" fully 35 of the 72 security patches it issued in 2002 and five of the nine security patches it has issued thus far in 2003.

The CLECs' arguments are a classic application of 20-20 hindsight, a standard of review which the Department has held is improper in assessing the prudence of a company's conduct. "A determination of reasonableness and prudence may not properly be made on the basis of hindsight judgments, nor is it appropriate for the Department merely to substitute its own judgment for the management of the utility. *Attorney General v. Department of Public Utilities*, 390 Mass. 208, 229 (1983). A prudence review must base its findings on how a company reasonably should have responded to the particular circumstances ... that were known or reasonably should have been known at the time the decision was made." *Boston Edison Company*, D.T.E. 98-119/126 at 62 (1999), *citing Fitchburg Gas & Electric Light Co.*, D.T.E. 98-51, at 12-13 (1998). *See also Boston Gas Company*, D.P.U. 93-60, at 24 (1993).

AT&T's argument that Verizon has failed to present a *prima facie* case entirely misses the point of *Boston Edison Company* and applies an improper standard here. AT&T Comments at 3-8. AT&T focuses solely on the MS SQL Server 2000 patch issued by Microsoft and argues that the Petition must fail because Verizon has offered no evidence that it "undertook the analysis or investigation necessary" to decide whether to install that particular patch. *Id*. at 5. Given the impossibility of "keeping up with" patches (even "critical" ones) and the current advice of security experts that damage control, not creation of an impenetrable defense, is the appropriate goal of computer security efforts, the issue here is not whether Verizon *could have* installed this particular patch but whether it reasonably could have *known that it should* install that patch, and that it should do so before installing other "critical" patches. If Verizon had had a crystal ball, and knew that the Slammer Worm was going to attack that specific vulnerability in Microsoft's SQL 2000 Servers slightly after midnight on January 25, 2003, it could have rearranged its IT operations and patch management to test and apply that specific patch to the vulnerable servers in advance of the attack. But Verizon did not have a crystal ball, and could not have known that among the multitudes of viruses infesting the Internet, a worm that exploited this particular defect in MS SQL Server 2000 would be unleashed and therefore that this particular patch should have been given such a super-priority. Thus, the only question for the Department to consider is whether Verizon acted prudently before the attack, by implementing reasonable procedures and systems to protect the network – and after the attack, by acting swiftly to limit the damage caused by the Worm. This, Verizon MA has demonstrated in abundance. *See* Petition at 3-8. The Department should not use 20-20 hindsight to require, in effect, that Verizon institute an absolutely foolproof patch management and cyber-security system that will predict – always and without fail – which viruses will attack and when.[3]

---

[3] The only state utilities commission that has yet ruled on Verizon's request for a waiver due to the effect of the Slammer Worm -- the Connecticut Department of Public Utility Control -- granted that request on March 28, 2003. *See* letter to William D. Smith dated March 28, 2003, in Docket No. 97-01-23. In Maryland, the Staff of the Public Service Commission recently recommended that the PSC grant Verizon's waiver request, on the condition that any future request for a waiver must be based on evidence that Verizon has taken "appropriate steps to inoculate its information systems from viruses …." *See* letter to Felecia L. Greer dated April 4, 2003, in Case No. 8916.

In any event, AT&T's claim that Verizon "did nothing in advance to address" the vulnerability ultimately exploited by the Slammer Worm, AT&T Comments at 8, is false. Verizon, Microsoft, CERT and other industry members were aware of several security vulnerabilities in MS SQL Server 2000. In this particular part of Microsoft's code, there were three known buffer overflow vulnerabilities and one weak permissions vulnerability about which Verizon and others were aware. In July 2002, Microsoft released a "stand alone" patch, designated as "critical" that addressed one of the buffer overflow vulnerabilities. That patch, however, left the other two buffer overflow vulnerabilities and the permission vulnerability open. Microsoft did not release Service Pack 3 (SP3), which corrected all of these defects (among others) and included the tools typically appropriate for patch installation, until almost six months later on January 17, 2003. Verizon had obtained SP3 and was in the process of evaluation and testing it when the Slammer Worm struck on January 25, 2003. Verizon had installed the patch on some of its devices before January 25, 2003, but as noted above, Microsoft itself admits that "it only took one machine" to let the Slammer Worm in.

NCI's suggestion that Verizon voluntarily shut down its wholesale interfaces in reaction to the mere "perceived threat" of the Slammer Worm, rather than an actual attack, has no basis in fact. As explained in the Petition, Verizon technical teams determined on January 25 that Verizon was in fact being attacked from the Internet and therefore quarantined parts of the system in order to ensure the safety of its own and its partners' networks. That quarantine process included shutting down connectivity paths to external entities, including the wholesale interfaces. *See* Petition at 4. Verizon's network does incorporate redundancy, as NCI states it should, but because of the nature of the Worm's attack, all connectivity paths to redundant network components were shut down.

NCI also suggests that other preventative measures should have been in place to protect Verizon's systems from attack. As fully laid out in the Petition, however, Verizon's security practices include the use of secure access infrastructure utilizing firewalls, ongoing security vigilance to detect and repudiate attacks, 24x7 network traffic monitoring, and 24x7 network device, server and system availability monitoring for critical systems. These measures and Verizon's vigilance in protecting its systems have repelled countless cyber attacks. *See* Petition at 9. Verizon participates in industry and government security information-sharing fora such as the NCC-ISAC and the Computer Emergency Response Team ("CERT") Coordination Center at Carnegie Mellon University. Verizon also has engaged the services of a third-party firm specializing in software security, which proactively notifies Verizon of impending cyber attacks. Unfortunately, these external groups were unable to warn Verizon in advance of the Slammer Worm attack. (In contrast, Verizon had one day's notice before the infamous CodeRed virus attack and 3 days notice before the Nimda virus attack.) In fact, Verizon was the first telecommunications company to notify the NCC-ISAC of the Slammer Worm attack.

Moreover, AT&T's carefully phrased assertion that the ATM, frame relay, hosting and voice services it provides to its own wholesale customers were not affected by the Worm is irrelevant. This was also true for Verizon. As we stated, it was Verizon's internal computing network that was affected, not its commercial networks. *Id*. at 5. What AT&T conveniently

fails to mention is that its *internal systems* were indeed infected by the worm, based on AT&T's responses to a post-attack inquiry by Verizon. AT&T also implies that Verizon's retail operations were not impacted. This is not true. Since the internal computing network was impacted by the Slammer Worm, both the wholesale and retail systems that use that computing network were impacted.[4]

NCI expressed concern that if this waiver request is granted that Verizon is likely to claim "worm" problems for any type of network issue. NCI's fears are unfounded. As noted above, since the PAP was instituted in New York in January 2000, Verizon has filed only one other PAP waiver request. *See* Petition at 8-9. Furthermore, the present waiver request does not seek general relief from complying with the PAP. Rather, the Petition states that the Slammer Worm affected only three pre-order measures out of hundreds of PAP measures. Verizon's performance on the remaining pre-order measures, ordering, provision and maintenance and repair measures was strong. In fact, as stated in the Petition, if the effect of the Slammer Worm was removed from the January PAP results, Verizon MA would not owe any PAP credits for January. *See* Petition at 1.

Finally, the CLECs' overblown claims that the Slammer Worm had a discriminatory, anticompetitive, or financial impact should be rejected. The Department and other state commissions have made it clear that the metrics in the PAP should be used to determine whether CLECs are receiving adequate service from Verizon. Verizon's performance is not evaluated on an incident basis, as the CLEC comments would imply. Instead, its performance is measured under the various standards and time frames in the PAP. A review of the numerous pre-order, provisioning and maintenance metrics included in the January 2003 PAP monthly report demonstrates that Verizon provided CLECs with exceptional service. In particular, Verizon provided excellent service on the fifteen (15) PO-1 "Response Time OSS Pre-Ordering Interface" submetrics that are included in the PAP. The same is true for February 2003. Indeed, the CLECs that have opposed Verizon's waiver have not claimed that they were attempting to access Verizon's pre-order systems on Saturday, January 25, 2003. NCI has offered no proof to support its entirely speculative claim that CLEC's "may have" lost large sums of money due to Verizon's protective actions in response to the Slammer Worm. NCI Comments at 2. In fact, only one CLEC notified Verizon that it was experiencing difficulty using a Verizon interface as a result of the network flooding caused by the worm. Thus, it does not appear that other CLECs were adversely affected in attempting to use Verizon interfaces on that Saturday afternoon. Although Verizon's electronic interfaces are available on weekends, ordering and provisioning requests received on Saturdays are treated as having been received on the next business day for

[4] For example, both wholesale and retail use that network to access the same back-end systems for ordering. *See* Carrier-to-Carrier Guidelines, Metric PO-2 "OSS Interface Availability" ("Verizon Service Representatives and CLEC Service Representatives obtain Pre-Ordering information from the same underlying OSS"). If anything, this incident highlights the better-than-parity service Verizon is required to provide to CLECs. The attack occurred on a Saturday, which is not considered "prime time" for Verizon's retail operations, but is considered as "prime time" for the purposes of calculating PO-2, even though experience clearly shows that Saturdays are not in fact high-use days by CLECs.

the purposes of providing services to the customer, which in this case was Monday, January 27, 2003. Moreover, despite some comments to the contrary (*see* WorldCom Comments at 3), press reports and Verizon's anecdotal information indicate that to the extent the systems of these CLECs relied on Microsoft's SQL Server 2000 and shared Internet-attached networks, they too were dealing with the fallout of the Slammer Worm on and after January 25, 2003.

* * *

No CLEC has established a valid basis to deny the request of Verizon MA for a waiver of certain service performance results for January 2003, that were adversely impacted by an Internet computer attack by a worm during the weekend of January 25, 2003. Verizon is vigilant in protecting the security of its physical and cyber assets and has repelled countless attempts to violate that security. Yet despite its best efforts, Verizon was unable due to the Slammer Worm to satisfy the service quality standards for the PO-2-02 metrics in the PAP for January 2003. Verizon MA has clearly established that the Slammer Worm attack was an extraordinary event, beyond Verizon's control. The claims to the contrary should be rejected, and the Department should grant the waiver request and allow Verizon MA to exclude the effects of the Slammer Worm from the monthly service results that will comprise the performance levels against which it will be measured under the PAP for January 2003.

Based on Verizon MA's strong showing in support of its Petition, if the Department is unable to issue a ruling on the Petition by April 18, Verizon MA will file the final January PAP report including the effects of the Slammer Worm, but Verizon MA requests that the Department stay Verizon's obligation to process the related credits pending the Department's decision on the Petition. If the Department allows the Petition, Verizon MA will re-file the January PAP report excluding the data for January 25, 2003. If the Department denies the Petition, Verizon MA will issue the credits and include interest thereon.

Respectfully submitted,

Bruce P. Beausejour

cc: Joan Evans, Esquire, Hearing Officer (3)
Michael Isenberg, Director – Telecommunications Division
Paul G. Afonso, General Counsel
Service List (e-mail)