Before the
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,	**)**	**D.T.E. 02-8**
into the collocation security policies of	**)**	
Verizon New England Inc. d/b/a Verizon	**)**	
Massachusetts	**)**	

REBUTTAL PANEL TESTIMONY OF COVAD COMMUNICATIONS COMPANY ON COLLOCATION SECURITY MEASURES IN MASSACHUSETTS

Panel:

Mr. Michael Clancy
Mr. Bart Shea

INTRODUCTION AND PURPOSE OF TESTIMONY

Q: PLEASE IDENTIFY THE NAME AND BUSINESS ADDRESS OF THE INDIVIDUAL PANEL MEMBERS TESTIFYING ON BEHALF OF COVAD COMUNICATIONS COMPANY IN THIS PROCEEDING.

A: The Panel consists of Mr. Michael Clancy and Mr. Bart Shea. Mr. Clancy's business address is 600 14th Street, N.W., Suite 750, Washington, D.C. 20005. Mr. Shea's business address is 1A Christine Avenue, Franklin, Massachusetts 02038.

Q: PLEASE BRIEFLY DESCRIBE THE EDUCATIONAL AND PROFESSIONAL EXPERIENCE OF EACH PANEL MEMBER.

A: The first Panel Member, Mr. Michael Clancy, currently is the Director of External Affairs for Covad Communications Company. In this capacity, Mr. Clancy acts as a liaison between Covad's business personnel and Verizon Communications on a variety of business and regulatory issues. Prior to his current position, Mr. Clancy performed customer support and operations functions for Covad in the New York tri-state region and was primarily responsible for building out Covad's network in New York as well as handling all other operations activities.

Before joining Covad in August 1998, Mr. Clancy worked for Verizon New York, Inc. and its predecessor companies, NYNEX and New York Telephone. He began his career as a Switching Equipment Technician and over a span of 27 years was assigned positions of increasing responsibility in Network Operations, Special Services and Network Engineering. In his last assignment at Verizon (then Bell Atlantic), he served as the Director of Network Engineering and was responsible for the provisioning of inter-office facilities networks and process management for the 14-state Bell Atlantic footprint. Mr.

Clancy obtained a Bachelor of Science in Business Administration from SUNY Empire State College in 1995.

The second Panel Member, Mr. Bart Shea, currently is the Senior EF&I Manager for Covad. In this capacity, Mr. Shea is responsible for deploying and maintaining capacity for Covad's collocation spaces in the Verizon North. In a previous position at Covad, Mr. Shea was responsible for turning up and maintaining Covad's central offices in the New England region. Before joining Covad, Mr. Shea was employed by GTE (formerly BBN and now Verizon) for 15 years, the last six of which were as the Field Services Manager for the Eastern Region. In that position, he was responsible for the installation and maintenance of GTE's Internet Network.

Q: WHAT IS THE PURPOSE OF THIS TESTIMONY?

A: The purpose of this testimony is two-fold. First, Covad seeks to directly address the issues raised by the Department in its *Vote and Order to Open Investigation* (*"Order"*) dated January 24, 2002 regarding the adequacy of current security measures with respect to existing collocation arrangements in Massachusetts. Second, Covad will rebut the Panel Testimony submitted by Verizon Massachusetts advocating that competitive carriers re-locate existing collocation facilities, and, in certain central offices, cede control of their facilities and equipment to Verizon Massachusetts via virtual collocation.

While the Department's inquiry is focused on the adequacy of those security measures in place with respect to access to Verizon central offices by competitive carrier personnel, the purpose of this proceeding is to ensure the continued network integrity and safety of *all* telecommunications networks, including the networks of competitive carriers. In

addressing the issues raised by the Department's Order, Covad's testimony will: (i) emphasize the importance of continued security with respect to all telecommunications networks, including the networks of Verizon and competitive carriers, and the necessity that any additional security measures be applied to all carriers on a non-discriminatory basis consistent with the Telecommunications Act of 1996 ("1996 Telecommunications Act"); (ii) denounce Verizon's attempt to expand the focus of the inquiry to security issues that *may* exist outside of the state of Massachusetts, such as its reference to an alleged incident in Brothel Washington, which Verizon has yet to substantiate as resulting from inadequate security measures or existing collocation arrangements, and the relevance of which Verizon has failed to demonstrate in this proceeding; and (iii) seek to extend the inquiry raised by the Department through an independent collaborative of subject matter experts from all affected carriers so that a more complete record of possible security issues can be established with industry wide recommendations for proceeding.

In rebutting the Panel Testimony submitted by Verizon Massachusetts, Covad will: (i) reiterate the Department's objectives in initiating this investigation and explain that the evidence produced by Verizon thus far fails to create any nexus between a clear and credible security threat and the security measures proposed; (ii) emphasize that Verizon's proposals regarding new collocation security policies are not a response to any real, substantiated security threat, terrorist or otherwise, but rather just another thinly veiled attempt to thwart competition in the market for facilities-based local services; and (iii) explain why Verizon's current proposals supporting virtual collocation exclusively in certain central offices and requiring separate entrances for physical collocation

arrangements in all others are (a) not reasonably related to the minimization or elimination of any real or perceived security threat, (b) discriminatory against competitive carriers through increased costs and operational inefficiencies, and (c) in direct contravention of the principles embedded in the Telecommunication Act of 1996 mandating physical collocation and efficient use of collocation space.

Finally, this testimony strongly urges the Department to defer any rulemaking that would create additional and unnecessary collocation rules and, in the alternative, encourages the Department, as set forth above, to establish an industry task force to identify potential security threats to the public telephone network and develop appropriate responses in that forum.

<u>THE FOCUS AND SCOPE OF THE DEPARTMENT'S INVESTIGATION</u>

Q: DOES COVAD BELIEVE THE DEPARTMENT'S INVESTIGATION INTO EXISTING COLLOCATION SECURITY POLICIES IS WARRANTED AFTER THE SEPTEMBER 11TH ATTACKS?

A: Yes. Covad believes the Department's effort to ensure a safe and reliable telecommunications infrastructure is both timely and warranted in the aftermath of the September 11th attacks. We believe that this investigation, if properly focused, will result in a more secure telecommunications infrastructure as required by the public interest.

Q: PLEASE EXPLAIN WHAT COVAD BELIEVES IS THE APPROPRIATE FOCUS OF THE DEPARTMENT'S INVESTIGATION.

A: The primary focus of the Department's investigation should be as stated in the *Order* -- to safeguard the Massachusetts telecommunications networks from tampering and thereby

ensure reliable telecommunications services to the citizens of Massachusetts. In adopting policies to limit telecommunications networks' vulnerability to terrorism, the Department's primary goal must be to promote the safety and security of *all* telecommunications networks in Massachusetts, including those of Verizon and the competitive local exchange carriers. In doing so, in addition to the questions posed in the *Order*, Covad believes the Department must examine (1) whether Verizon's collocation security policies need to be strengthened to safeguard competitive carriers' equipment and facilities located in Verizon's central office and (2) the nature and extent of access Verizon employees have to Verizon's central offices and other carriers' equipment to determine whether additional measures are needed to protect against potential tampering by such employees. The Department's inquiry must also examine effective ways to safeguard the entire telecommunications infrastructure and not just Verizon's central offices in the event of another attack. To truly protect the public interest, and minimize the impact of a terrorist attack, Covad believes the Department should focus on efficiently increasing the redundancy and reliability of the telecommunications infrastructure by facilitating the decentralized system of multiple facilities-based networks being built and operated by carriers other than Verizon.

Q: TO WHAT EXTENT SHOULD THE SCOPE OF THE DEPARTMENT'S INVESTIGATION BE LIMITED?

A: As an initial matter, the scope of this investigation should be limited to carrier activities and telecommunications infrastructure within Massachusetts. As previously stated, the Verizon Panel Testimony seeks to introduce an alleged "security violation" in Brothel, Washington as evidence that more stringent collocation security policies are needed in Massachusetts. The incident cited by Verizon, however, involves disputed facts, has yet

to be resolved and, frankly, is not relevant to this proceeding. As the Department is aware, states have varying collocation security policies and, consequently, the occurrence of a security breach in one state or central office does not automatically increase the likelihood that it will happen in another. In fact, the Verizon Panel Testimony admits that Verizon has "not experienced egregious and harmful security violations in Massachusetts," although it has in other states. *Verizon Panel Testimony* at page 21, lines 13-14. It is our view that the Department should strike the Brothel, Washington allegation from Verizon's testimony and direct the parties to limit the scope of their examination to infrastructure and carrier activities within the Commonwealth of Massachusetts.

Moreover, the Department must reject Verizon's attempts to redirect the focus of this proceeding from one that seeks practical solutions to identified security risks to one aimed at further limiting the rights of CLECs to independently operate their networks in compliance with current regulations. Rather than focus on determining whether existing security measures should be strengthened in response to the September 11th attacks, Verizon seeks to use this proceeding to rehash old arguments and reintroduce proposals previously rejected by the FCC and this Department. Not surprisingly, almost every collocation security measure proposed by Verizon would have the anti-competitive effect of limiting CLEC access to CLEC equipment located in Verizon's central office or significantly increasing the costs associated with collocation. The Department must not allow Verizon to use this proceeding as a pretext to thwart competition in the facilities-based local market. Despite Verizon's private agenda, all facilities-based carriers are equally susceptible to the devastation that would be caused by another terrorist attack

and, therefore, must work cooperatively to minimize the risks and potential damage of such an attack.

<u>COLLOCATION ARRANGEMENTS</u>

Q: PLEASE DESCRIBE COVAD'S COLLOCATION ARRANGEMENTS IN MASSACHUSETTS.

A: Generally, Covad has two types of collocation arrangements with Verizon in Massachusetts – caged physical collocation and cageless collocation open environment ("CCOE"). Both arrangements are considered "physical" collocation and provide Covad with necessary, around-the-clock access to its equipment and facilities in the event of routine maintenance and repair, a service outage or other customer emergency. In the past, Covad entered into virtual collocation arrangements with Verizon but, as discussed later, found this method of collocation to be inefficient and unreliable. As a result, we currently are converting all virtual collocation arrangements to CCOE.

Q. PLEASE EXPLAIN WHY COVAD PREFERS CCOE ARRANGEMENTS OVER VIRTUAL COLLOCATION ARRANGEMENTS.

A. CCOE arrangements are an attractive alternative to virtual collocation because they are cost and space efficient and provide Covad 24x7 access to equipment and facilities located in the ILEC central office. Unlike virtual collocation arrangements, CCOE arrangements provide Covad direct access to and control over its equipment and facilities for routine maintenance and repair and in the event of a customer emergency. Importantly, CCOE arrangements do not require that we cede control and ownership of our facilities to Verizon, a major competitor.

While there are no technical differences between CCOE arrangements and virtual collocation, virtual collocation historically has presented serious and sometimes insurmountable operational challenges for Covad. One major challenge is the management of collocation capacity. Under Verizon's own administrative rules, Covad must file an application each time it wants to augment existing collocation arrangements -- a process that usually takes Verizon 105 days to complete. Thus, every time Covad introduces a new service it must wait 105 days before the necessary collocation facilities are ready. Even a task as simple as rearranging cards in the DSLAM requires a new collocation application with Verizon, which means it will be at least another 105 days before the change takes place. Covad cannot always anticipate a change to customer services that far in advance. The extended processing period for collocation severely strains the optimization of the network and hampers Covad's ability to provide quality service.

For similar reasons, it is very difficult to manage assets under a virtual collocation arrangement. Once again, under Verizon's own administrative rules, any upgrade to the network hardware or firmware is considered a collocation augment triggering Verizon's 105-day application process. Usually, by the time the network upgrade is completed, the installed technology is obsolete requiring yet another upgrade. Verizon also requires CLECs to supply Verizon with enough maintenance spares for a single collocation arrangement to handle the constant upgrades and repairs to the telecommunications networks. It is not always possible to do this, which causes further delays.

Further, the maintenance services provided to CLEC equipment in a virtual environment are inadequate. While CLECs are required to pay for their own equipment maintenance, the service provided by Verizon is disorganized and generally poor. Verizon experiences significant turnover and reassignment among its technicians, which means that new individuals are constantly being trained at the CLECs' expense. Moreover, in Covad's experience, newly trained technicians often are so poorly trained or simply forget what they have learned that they sometimes require back-up from Covad personnel to complete a task. This is an added expense as Covad is required to pay both technicians. These higher costs ultimately are borne by the consumer which makes Covad's prices less competitive.

By converting its existing virtual collocation arrangements to CCOE, Covad will be able to eliminate many of the problems arising from its dependence on Verizon to perform collocation-related services. As with other forms of physical collocation, Covad will be able to: (1) monitor the types of services requested by customers and quickly add to the DSLAM to meet customer demands; (2) make faster upgrades to the network hardware and software; and (3) ensure that reliable, well-trained technicians are always available to maintain its equipment. Despite the obvious benefits, the transition from virtual collocation to CCOE has been unnecessarily delayed by Verizon's own administrative practices. In addition, Covad has been required to make very costly adjustments including: (1) the purchase of additional equipment to collocate in another, secured part of the central office; (2) filing a second collocation application; and (3) awaiting a full collocation interval (105 days) for site preparation and installation of additional security. These anti-competitive requirements imposed by Verizon have unnecessarily increased

the costs associated with collocation as well as resulted in significant delays in completing the transition.

Q: HAS COVAD IDENTIFIED ANY SECURITY CONCERNS IN MASSACHUSETTS RESULTING FROM ITS CURRENT COLLOCATION ARRANGEMENTS?

A: No. While Covad, like all facilities-based telecommunications carriers, remains concerned about potential security threats to its network, the company has not experienced any security breaches in Massachusetts to date. Similarly, the Verizon Panel Testimony indicates that Verizon also has not experienced any significant breaches in security in Massachusetts. The fact that two significant carriers in the Massachusetts telecommunications market have had no reports of material incidents involving security breaches or network tampering is a clear indication that the collocation safety policies currently in place are adequate and effective.

Q: WHAT FURTHER SECURITY MEASURES, IF ANY, SHOULD THE DEPARTMENT ADOPT TO ADDRESS POST-SEPTEMBER 11TH SECURITY CONCERNS?

A: At this point, Covad believes no changes are necessary until a more thorough review of existing security issues are examined. We believe the Department's focus should thus be on *examining* security matters rather than hastily requiring changes before all the facts are uncovered. As such, Covad strongly supports the *Motion* filed in this proceeding on April 25, 2002 recommending that the Department convene an industry task force comprised of security personnel from various carriers to first examine what security issues or risks actually exists. Only if the task force concludes that there are foreseeable and addressable security risks should amendments to the existing policies be considered.

As previously mentioned, the record thus far does not demonstrate a need for changes to the Department's existing collocation security policies as none of the parties has experienced serious security breaches which would justify the additional costs and operational inefficiencies that would likely result from any material amendments to such policies. If September 11th has taught us anything, it is that terrorists will use whatever means possible to cause the most damage and destruction to our people and information infrastructure, including our telecommunications networks. We, as carriers, must thus alter our thinking when it comes to securing our networks to take all reasonable measures against these massive assaults – whether from a plane that crashes into a central office or a truck full of explosives running into an RT– to ensure a redundant, fault tolerant communications infrastructure, both within Massachusetts and nationally. To focus the inquiry only on whether CLEC employees should have continued access to Verizon's central offices really fails to fully address the larger and more critical security concern. In this regard, through the participation of the industry task force, the Department must expand its inquiry beyond secured access for central offices. In addition, to the extent changes are ultimately made to existing collocation policies, such changes should focus on strengthening security measures meant to prevent unauthorized access to all telecommunications networks and infrastructure. This may be accomplished, for example, by improving personnel training, more comprehensive background checks for CLEC and Verizon employees and vendors, more effective and comprehensive use of "real time" security cameras and alarm monitoring technology, and greater efforts to ensure that only proper personnel/employees have access to the central offices and carrier facilities. It is these types of proactive measures that will ensure that only individuals

intended to be in the central offices have access to their companies' equipment, thereby minimizing a potential for terrorist infiltration of Verizon's central offices.

VERIZON'S COLLOCATION SECURITY PROPOSAL

Q: PLEASE COMMENT UPON VERIZON'S PROPOSALS FOR SECURING COLLOCATION FACILITIES.

A: As explained earlier, Verizon's proposed collocation security plan misses the point of the Department's investigation. Rather than introduce sound policies designed to minimize security risks introduced by potential terrorist attacks or network tampering, Verizon seeks to advance its long-term agenda of eliminating CLEC access to its central offices altogether. Specifically, Verizon's proposals seek to: (1) establish separate spaces for all forms of physical collocation (*i.e.*, separate rooms, floors, entrances and/or pathways) in order to secure and segregate the collocator's equipment from Verizon's; (2) relocate existing unsecured CCOE arrangements to secure or separated areas of the central office, space permitting, or otherwise convert them to virtual collocation; (3) provide CLECs with reasonable access to shared facilities outside the secured and segregated collocation space where partitioning of Verizon's equipment is feasible; (4) provide either virtual collocation and/or escorts for CRTEE arrangements; and (5) convert existing physical collocation arrangements to virtual collocation in action. Verizon claims that these proposed security measures are "appropriate, reasonable, in the public interest, and necessary to ensure the security, reliability and safety of Verizon's telecommunications network." *See Verizon Panel Testimony* at page 24, lines 3-6. Unfortunately, Verizon fails to demonstrate exactly how or why such proposed measures are "appropriate, reasonable and in the public interest."

A major flaw in Verizon's reasoning is that it has failed to provide a rationale for its proposals. Verizon goes on page after page proposing one new measure after another, but nowhere does it establish a nexus between any of its proposals and the security threats such proposals are supposed to prevent. Nowhere in its testimony does Verizon identify one threat, real or perceived, that justifies such sweeping changes. To the contrary, Verizon's Panel Testimony spends a significant amount of time identifying *potential* problems that *may* result from a CLEC employees' access to its network premises. No examples of security breaches in Massachusetts are cited and no explanation of how Verizon's proposals solve these *potential* breaches is provided. Indeed, the issues now raised by Verizon are the very same claims the FCC and this Department considered in previously rejecting measures similar to those proposed by Verizon in this proceeding. Although the security landscape has changed in the aftermath of the September 11th attacks, the Department's interest in protecting the integrity of the central offices is the same as before the terrorist attacks. Importantly, the Department's investigation does not suggest that CLECs pose a national security threat. Thus, unless and until Verizon puts forth a compelling explanation as to how its proposals will stop terrorist infiltration of a central office, they must be rejected.

Q: IN THE PANEL TESTIMONY, VERIZON STATES THAT THE MOST EFFECTIVE MEANS OF ENSURING NETWORK SAFETY AND RELIABILITY IS TO ELIMINATE PHYSICAL COLLOCATION IN CERTAIN CENTRAL OFFICES AND CONVERT THEM TO VIRTUAL COLLOCATION. DO YOU AGREE WITH THIS ASSESSMENT?

A: No. Let's be clear about Verizon's motives in this proceeding. It is Verizon's desire, as it always has been, to eliminate access by CLEC personnel to its central offices.

This objective clearly contravenes the requirements of the 1996 Telecommunications Act and Massachusetts law. Use of physical collocation is not merely some inconvenient option as Verizon suggests. Rather, the strong preference for physical collocation is embedded in the 1996 Telecommunications Act which requires ILECs to "provide, on rates, terms and conditions that are just, reasonable and nondiscriminatory, for physical collocation of equipment . . . at the premises of the local exchange carrier[.]" 47 U.S.C. 251(c)(6). This has been further borne out by the overwhelming majority of CLECs who prefer physical collocation over other alternatives so as to maximize control and efficiency over their own networks, thereby reducing costs to consumers. The only exception to this rule is where technical and space limitations prevent physical collocation. Thus, even assuming, *arguendo*, that virtual collocation slightly reduces the possibility of a terrorist threat, the elimination of physical collocation would require more than a petition to the FCC, but a statutory amendment by Congress. Unless and until it can be demonstrated that virtual collocation eliminates an actual serious security threat, such notion should be rejected.

In addition, Verizon's concerns about potential harmful acts by CLEC employees and vendors are overstated and unwarranted. First, as a general matter, CLEC employees and vendors gaining access to Verizon's central offices are subject to the same background checks as Verizon's employees and vendors. Thus, CLECs are no more likely to hire a potential terrorist than Verizon. Second, prior history indicates that Verizon-selected employees and vendors pose a greater security risk to Verizon's and CLECs' networks than do CLEC employees and vendors. In the past, especially during work stoppages and other labor disputes, Verizon-hired employees have deliberately sabotaged Verizon's

network. For example, in 1989 during a labor dispute, Verizon employees were arrested for sabotage and physical violence to Verizon's infrastructure. While these employees clearly pose grave security risks for Verizon and its network, many of these employees subsequently were granted amnesty, meaning they were immune to disciplinary actions. Incredibly, many of these bad actors were handed their jobs back without retaliatory action and no restrictive security measures imposed against them.

Converting existing physical collocation arrangement to virtual collocation fails to provide any real added security benefits that justify the enormous economic, operational, and administrative expense that would be incurred. These additional expenses would include, for example, Verizon's need to hire new employees to manage its central offices around the clock, the manpower and delay associated with a migration to, and use of, virtual collocation, and the administrative expense in amending current legislation to permit such regulatory adjustments. This enormous investment, which would be significantly borne by the CLEC community, is one that ironically likely increases the likelihood that a "sleeper terrorist" would gain access to a critical central office, as the inflow, and turn over, of Verizon technician employees would dramatically increase.

Q: VERIZON PROPOSES TO ESTABLISH SEPARATE ENTRANCES AND/OR PATHWAYS FOR ALL FORMS OF PHYSICAL COLLOCATION. DO YOU AGREE THAT THIS IS AN EFFECTIVE MEANS OF SECURING CARRIERS' TELECOMMUNICATIONS NETWORKS AND EQUIPMENT?

A: No. Requiring separate space and entrances for physical collocation arrangements would provide no tangible security benefits for the Massachusetts telecommunications infrastructure. Again, the CLEC employees are not the concern here. All facilities-based

carriers share the same concerns and interests in ensuring the safety and integrity of the telecommunications infrastructure. Verizon's Panel Testimony suggests that isolating Verizon's equipment from CLEC employees will somehow discourage terrorist attacks. There is no evidence to support this claim. To the contrary, the addition of more entrances and egresses only adds to the security risks as it increases individual access to the building. Moreover, the construction of separate entrances does little to protect the CLECs' facilities because even in a separate environment, Verizon's maintenance crew would still have access to such premises.

In addition, Verizon fails to demonstrate that separate entrances in this instance would be permitted under the FCC's rules. Pursuant to Section 51.323(i)(6) of FCC's rules, the ILECs may not construct or require construction of separate entrances unless the following conditions are met: (1) construction of a separate entrance is technically feasible; (2) legitimate security concerns exist; (3) construction of a separate entrance will not automatically delay collocation provisioning; and (4) construction of a separate entrance will not materially increase the requesting carrier's costs. 47 C.F.R. 51.323(i)(6). While it is probably technically feasible to construct separate entrances, the costs of doing so would undoubtedly increase CLEC expenses and delay collocation provisioning, which is inconsistent with the FCC's rules. Likewise, Verizon has not clearly identified any security concerns that would warrant the construction of separate entrances. The security concerns raised by Verizon again all point to the potential for CLEC tampering with ILEC equipment located in the central office, concerns that have not been borne out to date. Indeed, these concerns were considered and eventually dismissed by the FCC in promulgating its collocation rules.

Q: DO YOU AGREE WITH VERIZON'S PROPOSAL TO SEGREGATE CLEC EQUIPMENT FROM VERIZON'S?

A: No. Verizon's proposal to segregate CLEC equipment from its own provides no tangible security benefits to either party and will substantially increase CLECs' costs of doing business in Massachusetts. As previously stated, the purpose of this proceeding is to investigate security measures for the protection of Massachusetts's telecommunications infrastructure. That includes the networks of Verizon as well as other competitive carriers. Segregating Verizon's equipment from other carriers does nothing in the way of reducing the risk of terrorist attack, but only increases the costs and inefficiencies surrounding collocation.

Again, there is no mention of security measures that would protect CLECs from harmful acts by an angry or disillusioned Verizon employee. Verizon simply fails to understand that on the issue of network security all carriers are on the same side. No carrier wants to risk the security and integrity of its network to acts of terror or vandalism by third parties. Consequently, any efforts to truly deter such activity must result from a cooperative effort of all parties involved.

Q. IN ITS PANEL TESTIMONY, VERIZON STATES THAT CCOE ARRANGEMENTS PRESENT A SECURITY RISK TO ITS CENTRAL OFFICE FACILITIES. DO YOU AGREE?

A: No. Verizon's concerns are unsupported. Once again, Verizon fails to provide any evidence that CLECs pose a risk to its equipment and facilities. CCOE arrangements do not present an added security risk just because they are located in an area where other

Verizon equipment is located. As stated before, CLECs, who are dependent upon ILECs for certain facilities and services, have no interest in tampering with or destroying ILEC facilities. Indeed, such carriers have every reason to ensure the integrity of the Verizon network. If anything, the CLECs should be concerned about an unscrupulous ILEC employee intentionally or unintentionally tampering with their equipment and disrupting customer service. As previously noted, CLEC technicians, the apparent source of Verizon's security concerns, are subject to background checks by both their CLEC employers *and* Verizon. While we know there are no guarantees, this practice is probably the most reliable way for CLECs and Verizon to detect potential terrorists in the ranks.

In important ways, CCOE arrangements provide higher levels of security from tampering and terrorists activities as the foot traffic in the central office is likely to be greater than with other collocation arrangements. With more people around from different companies, it is highly unlikely that any carrier's' employee will tamper with another carrier's equipment for fear of being caught and subsequent reprisal. Further, Verizon's "fear" that CLEC employees will work on the wrong shelf or equipment is unfounded. To the extent there is a problem, the reason must be that Verizon's current identification measures are inadequate, not that a CLEC's employees would inadvertently or intentionally work on the wrong equipment. This is a simple fix.

Q. PLEASE COMMENT ON VERIZON'S PROPOSAL THAT THE DEPARTMENT NOT REQUIRE PHYSICAL COLLOCATION AT COMPANY REMOTE TERMINAL EQUIPMENT ENCLOSURES ("CRTEE").

A: Verizon's concerns are premature since, as Verizon admits, there currently are no RT arrangements in Massachusetts. Once again, Verizon seeks to have the Department impose more restrictive security measures on CLECs even where there is no evidence of a security risk. Absent its speculative analysis, Verizon fails to adequately explain the potential security risks that exist from physical collocation arrangements in RTs. As far as Covad can tell, Verizon appears to think the size of RTs present the most serious consideration. If RTs are such great security risks due their small size, then perhaps Verizon should reconsider their use at all. In the final analysis, security at RTs should be handled no differently than at central offices, with the same rights of access and collocation.

Q: PLEASE COMMENT ON VERIZON'S PROPOSAL TO ELIMINATE ACCESS TO COMMON AREAS WHERE SEPARATE BARRIERS CANNOT BE ERECTED AROUND VERIZON'S EQUIPMENT.

A: Verizon's proposal seeks to provide access to such facilities only where convenient. Access to shared facilities, however, is not an "optional" service as Verizon suggests. Rather, Verizon is required to provide access to common areas such as restrooms, loading docks and elevators by FCC and OSHA regulations, and, thus must continue do so even when it cannot separate or secure its equipment from common areas. Moreover, Covad disagrees with Verizon's assertion that escorts are needed to accompany CLEC employees and vendors accessing shared facilities, at least to the extent CLECs would be required to absorb the costs. As this Department and the FCC have determined in the

past, it is an unnecessary measure that only increases the need for additional manpower and drives up the cost of doing business.

Q: WHAT STEPS MAY VERIZON REASONABLY TAKE TO PROTECT ITS FACILITIES AND EQUIPMENT?

A: The FCC rules and regulations and Department orders outline the various security measures that may be used by Verizon and other carriers to protect facilities and equipment located in Verizon's central offices. As stated earlier, these measures have proven quite effective in Massachusetts as there has been no significant incidents of security breaches. The measures available and currently used by Verizon include: (1) use of security cameras in the central office; (2) computerized personnel badges to be used to gain access to the central office; (3) security training for all employees and vendors; and (4) physical separation of carrier equipment, where necessary. All of these security measures have proven adequate to protect Verizon's central office from security breaches in the past and certainly remain adequate to prevent the *potential* lapses identified by Verizon in this proceeding.

Because the costs of any additional security measures inevitably will be borne by the CLECs, there must be a direct nexus between a "real" and significant security threat and the additional security measures proposed by Verizon. In addition, any proposals adopted should be narrowly tailored to address real and significant security issues and must be the least expensive, effective alternative available.

It is incumbent upon the Department to ensure that Verizon does not use this proceeding to circumvent existing collocation obligations and increase the CLECs' costs of doing

business. These measures are in place to protect the interests of competitive carriers and ensure the proliferation of facilities-based competition. The security collocation policies in place thus far have proved adequate to protect Verizon's and CLECs' central office facilities from security breaches and harmful attacks. There is no reason to amend these rules absent a compelling security risk, which has not been demonstrated in this proceeding.

Q. DOES THIS CONCLUDE YOUR TESTIMONY?

A. Yes.

DC01/EDMOA/182735.1