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**

PANEL SURREBUTTAL TESTIMONY OF VERIZON MASSACHUSETTS

Members of the Panel:

Lawrence R. Craft
Francesco S. Mattera
Lynelle Reney
Peter Shepherd

June 18, 2002

I. THE WITNESS PANEL

Q. Please identify the name of the individual panel members who are submitting this surrebuttal testimony on behalf of Verizon Massachusetts ("Verizon MA").

A. The members of this panel, Mr. Lawrence R. Craft, Mr. Francesco S. Mattera, Ms. Lynelle Reney, and Mr. Peter Shepherd, are the same persons who filed Verizon MA's initial panel testimony in this docket.

II. PURPOSE OF TESTIMONY

Q. What is the purpose of this surrebuttal testimony?

A. In this surrebuttal testimony, Verizon MA responds to the testimony filed by AT&T, WorldCom (WCOM), Covad, Qwest, Allegiance, and Sprint on May 15, 2002. Specifically, Verizon MA (1) explains that these parties, in general, seriously underestimate the potential security risks in today's environment; (2) shows that the parties misunderstand or mischaracterize Verizon MA's collocation security proposals; (3) rebuts the other parties' criticisms of Verizon MA's proposals; and (4) shows that to the limited extent that the other parties have made concrete recommendations of their own, those recommendations are inadequate or inappropriate.

III. INHERENT SECURITY RISKS ASSOCIATED WITH PROVIDING UNRESTRICTED ACCESS IN VERIZON MA's CENTRAL OFFICES

Q. Do you agree with the assertions of other parties that Verizon MA has not identified security risks associated with collocation?

A. No, we do not.

Q. Why not?

A. The current requirements for providing other carriers access to collocation space in incumbent LECs' central offices were established by the Department and the FCC prior to September 11, 2001. These requirements include providing physical, cageless, and virtual collocation arrangements; 24 hour access to those facilities without the need for escorts; and reasonable access to other shared facilities such as loading docks, elevators, temporary staging areas and restroom facilities. Those requirements were established in the past, under different circumstances. *Vote and Order to Open Investigation,* at 1, 6-7. Given the critical importance of telecommunications and the heightened concern over security, it is critical to re-examine those requirements in light of the risks those requirements raise.

Q. What are the principal risks associated with the existing collocation requirements?

A. The potential security risks are associated with other carriers having unrestricted access to or through Verizon MA's equipment areas.

Q. Please describe why unrestricted access is a problem.

A. Once access of any sort is given – even authorized access – there is greater "foot traffic" in the central offices which potentially exposes the network infrastructure to a greater degree of risk.

Q. Surely Verizon MA is not accusing CLEC employees of being terrorists or "predisposed to committing terrorism," to use Qwest's phrase (Qwest Testimony at 7)?

A. Verizon MA is not making any such claim. What we are saying is that while the security breaches in Massachusetts and elsewhere are not in the nature of terrorist acts, they were the result of other carrier personnel and their vendors having access to Verizon central offices in connection with collocation. They illustrate the potential risks and harm, including *potential* disruptions to service, and provide useful information concerning potential ways in which telecommunications in America could be disrupted. Moreover, the Department's inquiry is not limited to the prevention of acts of terrorism. The Department is also concerned about enhanced security measures that may be warranted as proactive preventative steps to help deter inadvertent or intentional incidents that could disrupt service, that are linked to current collocation policies and Verizon MA security procedures related to providing collocation.

Q. Does Verizon MA contend that its proposal will eliminate all risks of security breaches?

A. No. As already described in Verizon MA's Direct Testimony, no degree of collocation security measures can provide absolute protection against a potential physical attack against telecommunications facilities, or the efforts of misguided Verizon employees, collocators' employees, or their contractors or vendors determined to harm the telecommunications facilities from within. Verizon MA's proposal attempts to reduce these risks.

Q. Please comment on the other parties' arguments that Verizon MA has not provided evidence of security issues specific to Massachusetts, and that therefore there is no evidence that change is necessary (e.*g.*, Allegiance Testimony at 3; Sprint Testimony at 9; Qwest Testimony at 5, 8).

A. While evidence of incidents in Verizon MA's central offices may be less than in other jurisdictions (and is likely influenced by the manner in which Verizon MA has designed its collocation space, as explained in the following sections) that does not mean that we should ignore the need for greater security measures. Verizon MA's proposed plan addresses the security concerns of access to its central offices by other carriers that is a preventative measure to deter potentially harmful incidents and events that may disrupt service.

Q. Should the Department ignore those problems because they did not occur here?

A. No. It would be unwise not to consider problems that have occurred in other states, especially where harm has resulted in service outages. In other states, security violations have resulted in damage or theft of costly equipment. These incidents highlight once unrestricted access is provided, the security risks and likelihood of harm (including but not limited to acts of terrorism) increases.

Q. Is it appropriate to wait until the network infrastructure in Massachusetts experiences harm before addressing the issue here?

A. No. The purpose of the Department's investigation, and the thrust of Verizon MA's collocation security proposal, is to identify and consider additional proactive and

preventative measures that increase the security of the Massachusetts network infrastructure and as a result contribute to public safety and welfare. The Department's objective is to be prepared for events that *may* occur in Massachusetts. Limiting access to certain critical buildings and to critical areas that should not be accessed by other carriers is the most effective and efficient means "to safeguard telecommunications networks from tampering and thereby to ensure reliable telecommunications service to the citizens of Massachusetts" (*Vote and Order to Open Investigation* at 1), because it minimizes the opportunity for harmful acts to the network.

Q. Do you agree with AT&T that cyber or electronic sabotage or physical attacks upon power or water supply facilities are more likely than attacks upon telecommunications facilities (AT&T Testimony at 8, 18-19)?

A. No. No one can predict with certainty where acts of sabotage will occur. On "NBC Nightly News" for May 28, 2002, it was reported that one problem for security experts trying to guess where terrorists will strike next is the sheer number of potential targets in the United States. National security experts believe telecommunications infrastructure facilities as well as other infrastructure facilities are potential targets. For example, Attorney General Ashcroft told the media on October 8, 2001, that the FBI had issued warnings through the National Threat Warning System to law enforcement agencies and more than 27,000 corporate security officers at companies that own and operate systems, including telecommunications infrastructure systems, to prepare for a new wave of attacks. In addition, on October 4, 2001, John Tritak, Director of the U.S.

Commerce Department's Critical Infrastructure Assurance Office said in a statement to the Senate Government Affairs Committee, "That the loss of telecommunications services can impede financial service transactions and delivery of electric power is no longer an exercise scenario. There can be no e-commerce without 'e' – electricity. There can be no e-commerce without e-communications."

Q. Qwest claims (pp. 9-11) that neither the Department, nor Verizon, can hope to secure central offices against terrorist threats by merely restricting access by CLEC personnel. Do you agree?

A. Not entirely. As discussed above, Verizon MA does not contend that its security proposal will prevent all attacks by terrorists against telecommunications facilities or efforts by misguided employees, collocators, or their contractors or vendors to harm those facilities from within. However, restricting access within the central offices, and to certain critical central offices, is a very significant step in reducing the risk of inadvertent or intentional harm to these facilities. Preventing 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. Restricting access to Verizon MA's equipment lessens the probability that an inadvertent or intentional action will harm the network by reducing the potential numbers of individuals that have access to that equipment.

IV. EFFECTS OF VERIZON MA'S PROPOSAL ON CURRENT COLLOCATION PRACTICES

Q. Please describe how the other parties have misunderstood or mischaracterized Verizon MA's proposal.

A. The other parties have misunderstood or mischaracterized Verizon MA's proposal in a number of ways, among them by (1) suggesting that Verizon MA's proposal represents a radical change from current practices and (2) by mischaracterizing the proposal as Verizon MA's anticompetitive attempt to burden CLECs with unnecessary requirements and costs.

Q. Please explain why Verizon MA's proposal is not a radical change from current practice.

A. As noted on page 23 of our initial panel testimony, Verizon MA proposes the following five steps: (1) establishing, for all forms of physical collocation (caged and cageless) space for collocation and access to that space in a manner that maintains a physical barrier that prevents access by other carriers to or through areas containing Verizon MA equipment (*e.g.*, separate rooms, floors, entrances and/or pathways to such areas); (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. With the exception of Item 5 (the designation of critical COs), which will be discussed later in this testimony, the other four requirements are for the most part already in place and followed today in Massachusetts. Verizon MA's collocation security proposal would retain many of Verizon MA's current policies, and further enhance them as described in our previous testimony to meet the heightened security needs in today's environment.

Q. Please explain how Verizon MA has assigned physical collocation space in central offices up to this point?

A. As a general rule, when assigning and designing collocation space for other carriers in its central offices, Verizon MA's engineers generally try to create collocation areas in space where there is no access to Verizon's own equipment areas or where Verizon MA can create a secured partition between its own equipment space and the collocation space. That is, access to Verizon's equipment area(s) by other carriers, once they have entered their collocation area(s), is constrained by a wall, or in some cases a wire mesh partition, separating Verizon's equipment area from the collocation area. Entry to the Verizon equipment area is possible only through locked doorways. Access to the collocation area(s) is by means of secured corridors where access to Verizon's equipment area(s) is also constrained by walls or in some cases a wire mesh partition with locked doors that other collocated carrier's building key or CRAS access card will not open.

Q. Please describe how entrances to central offices are commonly laid out with regard to collocation space.

A. Although there are generally common entrances into Verizon MA's central offices, they lead in many cases to a hallway or corridor from which collocated carriers would then proceed to their physical collocation arrangements.[1] The pathway is generally separate from Verizon MA's equipment – *i.e.*, at a minimum, it is secured by walls or in some instances mesh partitions that separate the ingress/egress route and Verizon's equipment area(s). Likewise, in Verizon MA's multi-story central offices equipped with elevators, the elevator is generally near the entrance or the secured hallway, and takes the collocated carrier to the appropriate floor of the central office for the physical collocation arrangement. If the collocated carrier inadvertently or intentionally takes the elevator to the wrong floor, the carrier's key or access card will not open locked doors leading to Verizon's equipment area(s). Once on the appropriate floor in a Verizon MA central office, the carrier's keys or access card will only open the door to the space where the collocation arrangement is located. Thus, no change is required in existing collocated central offices.

[1] WorldCom incorrectly claims that Verizon MA provided separate entrances for CLEC personnel during work stoppages because of concern with potential Verizon MA employee misconduct (WorldCom Testimony at 12). During periods of work stoppage it is a common procedure, where possible, to designate separate entrances for non-affiliated occupants and tenants of the facility and occupants affiliated with the firm whose bargained for members are engaged in a labor dispute, for purposes of lawful picketing, so as to minimize disruption to the non-affiliated occupants operations. The Department has approved the practice of designating separate entrances for use during work stoppages. *Vote and Order to open Investigation* at 5.

Q. Where in Massachusetts does Verizon MA currently provide segregated collocation space?

A. All physical collocation arrangements are currently in segregated space, with the exception of one in-service CCOE physical collocation arrangement in the Hopkinton central office.

Q. What effect would adoption of Verizon MA's proposals regarding segregated collocation space have on existing collocation arrangements?

A. Except for the Hopkinton central office, it would not be necessary to modify any existing collocation arrangement. In Hopkinton, the building configuration would not permit construction of a separated collocation area. Therefore, under Verizon MA's proposal, the one in-service arrangement in that office would be converted to a virtual collocation arrangement.

Q. What effect would Verizon MA's proposed requirement of segregated collocation space have in the future?

A. On a going forward basis, Verizon MA would continue to locate physical collocation arrangements in separated space. In addition, Verizon MA seeks the ability to close a central office to physical collocation if secured segregated space cannot technically be made available. This would enable Verizon MA to limit future cageless collocation arrangements to only those central offices where Verizon MA has or can provide secured segregated space. In fact, this is consistent with the Department's previous

decision in D.T.E. 98-21 (*Covad Communications Company*), which did not permit unsecured cageless collocation arrangements in Massachusetts.

Q. Please comment on Sprint's claim (p. 9) that if cageless collocation were not an acceptable security risk, the FCC would not expressly permit it.

A. Verizon MA is not proposing to eliminate all cageless collocation, but only cageless collocation in areas that cannot be physically separated from Verizon MA's equipment areas. Moreover, the FCC's requirements predated the events of September 11th. The Department is legitimately examining the risks associated with those requirements post-September 11.

Q. Regarding Verizon MA's proposal for CLEC access to common areas, how does Verizon MA's proposal differ from current practice?

A. Verizon MA's proposal would maintain its current policy of 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. Prior to the Department's initiating this investigation, there were no objections from collocated carriers to this longstanding Verizon MA practice. This practice is appropriate and reasonable, especially with heightened security concerns in today's environment, and should be continued. In addition, Verizon MA proposes that if 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. This is consistent with the FCC's requirements that permit reasonable access (not "unlimited" access) to such shared facilities.

Q. Is Verizon MA's proposal regarding escorted access or virtual collocation in remote terminals consistent with current practices? Please explain.

A. Yes. First, Verizon MA has not received any request for remote terminal collocation and there are no other carriers collocated at any remote terminal in Massachusetts. Thus, Verizon MA's proposal regarding remote terminals and RTEEs will not affect any existing collocated carriers.

Q. Are remote terminals provisioned with secured, separated space for collocated equipment?

A. No. Verizon MA uses three basic forms of remote terminal enclosures for digital loop carrier circuit equipment that is located remotely from the central office. They are: (1) controlled environmental vaults ("CEVs") below ground structures that provide control over temperature and humidity conditions; (2) controlled environmental huts (similar to CEVs but above-ground structures); and (3) cabinets which are above-ground, non-environmentally controlled structures mounted on a pad, wall or pole. CEVs and huts often are only large enough for a single technician to enter and gain access to equipment and wiring in the limited space available. A technician gains access to cabinet enclosed equipment and wiring from outside the structure through a hinged door opening. Remote terminals are engineered, prefabricated and pre-equipped to accommodate Verizon MA's equipment requirements, generally for a three-year planning period, and

are completely pre-wired for the maximum capabilities that can be provided from that terminal. Therefore, unlike a central office, they cannot be practically retrofitted or rearranged to accommodate the physical collocation of another carrier's equipment.

Q. Is it practical to equip remote terminals with electronic card reader access systems?

A. No. Currently access to remote terminal equipment enclosures is secured by various means such as padlocks, keyed doors or the use of special tools. Retrofitting these structures with more costly electronic card reader access systems to give other carriers access to the enclosure is not a practical solution.

Q. Do you agree with AT&T's claim that escorts are not necessary for RTs from the standpoint of security, nor are they permissible under current FCC rules (AT&T Testimony at 29)?

A. No. First, if the Department does not accept virtual only arrangements as a reasonable security measure, then escorts are necessary due to the nature of these small pre-equipped and pre-wired structures with limited space that precludes the separation and securing of each carrier's equipment. Second, this issue is still under consideration at the FCC. In its Second Notice of Proposed Rulemaking in CC Docket No. 98-147 and CC Docket No. 96-98 (FCC 00297), the FCC sought comments on issues related to collocation at remote ILEC premises and in particular, whether virtual collocation constitutes an acceptable replacement for physical collocation at remotes. The FCC has not yet completed this phase of its proposed rulemaking or established final rules on this issue. Finally, current FCC rules do not prohibit this approach.

Q. Is the fifth step in Verizon MA's security plan regarding identifying critical offices already in existence today?

A. No. The last step in Verizon MA's proposed security plan to establish criteria for designating a limited number critical central offices as available only for virtual collocation and converting existing physical collocation arrangements to virtual collocation in those selected, high security risk central offices is not in place today.

V. "VIRTUAL ONLY" CRITICAL CENTRAL OFFICES

Q. Does Verizon MA consider the designation of certain COs as "critical," and thus subject to virtual collocation only, essential for security purposes?

A. Yes. In addition to the security measures previously described, the designation of certain critical COs is a reasonable and necessary component of Verizon MA's proposed plan. As demonstrated above, the increased number of additional personnel of other carriers accessing these locations, increases the opportunity or chance that inadvertent or intentional actions could harm those critical network facilities. These critical offices require the additional degree of security that eliminating physical collocation would provide.

Q. What factors should govern which central offices are "critical" CO under Verizon MA's proposal?

A. As noted in our prior testimony, these factors include whether accidental or intentional damage to the network resulting in disruption of existing service in particular central offices could pose national security risks, endanger the health, safety and welfare of

many more lives, and jeopardize the operations of major businesses, public safety, and government agencies, as well as advanced technology companies and other institutions that are involved in national security matters. The presence of an access tandem, E911 control tandem, or a Signaling Transfer Point (STP) in a central office influences whether that central office should be deemed critical. Additionally, certain central offices may be critical if they house facilities used to serve critical entities (*e.g.*, nuclear facility or a major airport facility).

Q. Why are these factors important in assessing whether a central office is critical?

A. Failure of these facilities has the potential to significantly disrupt critical communications, jeopardizing public safety and national security.

Q. Let us discuss these facilities in turn. Why is an access tandem important?

A. An access tandem is or can become a single critical point of failure in Verizon's network. In Massachusetts, an access tandem functions as the hub for many inter-office toll routes and as the final route for all other local and toll interoffice traffic when other routes are unavailable. In addition, many interconnectors including CLECs and IXCs rely on an access tandem to access Verizon's network. The loss of an access tandem would lead to an unacceptable blockage of toll traffic, and has the potential to isolate interconnecting carriers who interconnect at the access tandem.

Q. Why would the presence of an E911 control tandem or signaling transfer point (STP) make a CO critical?

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

Q. How will the determination of which COs are critical be made?

A. As set forth in our original panel testimony, Verizon MA would work with the Department to assist the Department in determining which specific COs are critical.

Q. Is Allegiance's allegation on page 8 of its testimony, that Verizon MA's proposal is "well on its way to eliminating physical collocation entirely," correct?

A. No. Allegiance misunderstands Verizon MA's proposal. Verizon MA would restrict to virtual collocations only a limited number of central offices deemed to be "critical" to overall network functionality, national security, the public safety, health, welfare and economic interest of the general public. It would not eliminate all physical collocation.

In critical central offices, Verizon MA would continue to provide collocation by converting in place existing physical collocation arrangements to virtual arrangements, thereby providing a viable means for other carriers to interconnect for the exchange of traffic and access to Verizon MA's unbundled network elements.

Q. Various parties allege problems with virtual collocation, especially in other jurisdictions. Please respond.

A. We disagree with these allegations. As the Department is aware, there have been few complaints regarding Verizon MA's performance related to virtual collocation. In fact, when Rhythms raised performance issues in connection with Verizon MA's virtual collocation performance during Verizon MA's § 271 inquiry, the parties, at the direction of the Department, successfully investigated and resolved the problem. Attachment 1 is the joint letter by Rhythms and Verizon MA regarding this issue filed in the Verizon MA § 271 matter.

Q. Please respond to Covad's claims that "every time it introduces a new service it must wait 105 days before the necessary collocation facilities are ready." Covad Testimony at 8.

A. This is incorrect. Covad appears to be referring to the interval for the *establishment* of a new virtual collocation arrangement, which is actually 76 days and is the same as for a physical arrangement. Once the arrangement is established, a CLEC would order individual services in accordance with the applicable tariff intervals and can control the time frame in which to offer new services to its customers.

Q. Is WorldCom (at 9) correct that CLECs must incur considerable expense retraining Verizon MA to maintain and repair virtually collocated equipment?

A. No. Verizon MA, not the virtually collocated carrier, is responsible for re-training Verizon MA's technicians. Additionally, the collocated carrier is only responsible for the initial training if the virtual collocation equipment is not equipment that Verizon MA's technicians are already familiar with and trained to maintain.

Q. Some parties raise concerns regarding the transition to convert physical to virtual (WorldCom Testimony at 23-24; Allegiance Testimony at 2; Covad Testimony at 16). How would Verizon MA ensure and prevent CLEC customer outages?

A. In COs where physical arrangements would be converted to virtual arrangements (such as the one arrangement in Hopkinton or in central offices that may be designated as critical), the existing CLEC equipment would be converted to virtual collocation in place. There would be no physical relocation of equipment or conversion of circuits, and hence, no disruption of the affected customers' service.

Q. If existing CLEC physical collocation arrangements are converted to virtual arrangements under Verizon MA's proposal, should, as Allegiance suggests, Verizon MA refund the difference between the nonrecurring charges CLECs have already paid for physical collocation and the nonrecurring charges they would have paid for virtual collocation?

A. Verizon would handle any adjustments of nonrecurring charges in accordance with applicable tariffs.

Q. Please address AT&T's recommendation that the Department establish additional performance metrics, penalties and reporting requirements (AT&T Testimony at 23).

A. Verizon MA believes the NP-2 measurements already established in the Carrier to Carrier Guidelines for collocation performance, which include Virtual – New and Virtual - Augment metrics are adequate. Additional metrics as suggested by AT&T should not be required and would be an added unnecessary regulatory burden.

VI. DISCUSSION OF ALTERNATIVE SECURITY MEASURES, INCLUDING THOSE UTILIZED BY OTHER CARRIERS

Q. Have the other parties offered any proposals of their own to enhance the security of Verizon MA central offices?

A. Only to a limited extent. Although most of the parties claim that Verizon MA's collocation security proposal goes too far, they offer few alternatives. WorldCom and Covad, for example, advocate maintaining the status quo (WorldCom Testimony at 27-30; Covad Testimony at 21). AT&T suggests that improved implementation of current security measures, such as improved entry procedures, card readers access systems, and security cameras, is more appropriate (AT&T Testimony at 6).

Q. Please respond to Sprint's claims: that at least 80% of the security violations will not be cured if Verizon were to implement its security measures and that 40% of total incidents involved break-ins, thefts, violations and service interruptions and harm to CLECs, not Verizon MA; that only 19% of the security violations have anything to do with CLECs

having access to the ILEC central offices; and that most of these incidents are not network threatening (Sprint Testimony at 8).

A. It is difficult to respond to Sprint's conclusory statements. While most of the incidents at Verizon facilities may not have resulted in immediate and measurable threats or impacts on the network, the incidents do point out that the presence of other carriers in Verizon's central offices for collocation have produced more instances of security breaches than if they did not have access to those buildings or access to unauthorized areas within the buildings. At least one incident, although not in Massachusetts, did result in a major disruption to service such as the Department's inquiry is seeking to prevent.

Q. Do you agree with Qwest's claim that Verizon MA is not appropriately implementing existing security measures at its central offices (Qwest Testimony at 19, 22, 23).

A. No. Qwest is incorrect that Verizon MA's efforts to implement existing security measures should be improved before looking at any additional measures. Verizon MA takes the security of its facilities and provision of reliable service very seriously and has implemented and administered its security practices vigorously and diligently.

Q. Please explain why the limited security enhancements suggested by some parties (*e.g.*, dummy and live cameras, stricter control of ID badges, and electronic access key cards) are insufficient.

A. These measures would be useful in combination with more limited CO access, but they are not sufficient in themselves as an alternative to access restrictions.

Q. Please respond to AT&T's claim that Verizon MA does not currently use cameras effectively to monitor and prevent undesirable conduct (AT&T Testimony at 14) and Sprint's claim that additional closed-circuit TV (CCTV) systems in Verizon MA's most populous central offices would be adequate (Sprint Testimony at 13).

A. CCTV systems have been deployed in locations where conditions justify their placement, such as where other carriers potentially have access to or through Verizon MA's equipment space. Although deployment of additional cameras and similar equipment can provide a degree of enhanced security, CCTV will not deter all individuals from committing criminal acts. For example, dummy cameras are not likely to deter individuals who are authorized to enter the central office but who intend to harm the network once they gain access. Likewise, even real-time CCTV monitoring will not guarantee security in central offices because not all areas can be covered and not all activity can be captured due to the physical configuration of equipment and space in those locations. Therefore, while real-time monitoring may act as a deterrent for some individuals, it will not necessarily prevent an attack once the perpetrator is inside a Verizon MA central office. Placing additional limits on central office access is a necessary first step to ensure a greater degree of central office security.

Q. Please describe Verizon MA's deployment of keyed and electronic Card Reader Access Systems ("CRAS") in Massachusetts.

A. Currently, access to all central offices is through secured entrances that are either manned by contract guard service or by locked doors, opened by means of a key or

electronic CRAS. Within the central office, access to almost all collocation areas is also through locked entries – opened either by a key or card reader access. Access to Verizon MA's equipment areas, except as noted previously for the Hopkinton central office, are also through secured locked entrances opened by means of a key or card reader access. Verizon MA's proposal is an extension of this approach in use today. Keyed or card reader access alone is not enough since collocated carriers have not consistently followed and do not always diligently follow Verizon MA's policy of returning authorized badge or electronic card reader access cards when an employee has terminated employment with the collocated carrier, or reporting stolen or lost cards on a timely basis (if at all).

Q. Please respond to Qwest's allegation that Verizon does not seem to be using any mechanisms available to protect against misappropriation of cards, and that Verizon MA does not keep track of which of its employees have keys to its central offices, how many electronic access cards it has issued, or to whom those cards were issued.

A. Verizon MA has established effective procedures for its own employees and vendors, as well as procedures for submission of applications for collocated carrier employee and vendor access to central offices, the issuance of electronic access cards and building access keys, and tracking who has been provided cards and keys. These procedures were described in our prior testimony. Verizon MA effectively and diligently follows these procedures. In contrast to the control it has over its own employees and vendors, Verizon does not have control over how other carriers

administer their own internal procedures to ensure that their employees or vendors properly use and protect the use of access cards, prevent the inappropriate use of another individual's access card, and ensure that building access keys are guarded and properly distributed and returned by employees or vendors.

Q. Please comment on AT&T's claims that Verizon MA should implement electronic card reader systems that register card swiping on entrance *and exit* (AT&T Testimony at 14).

A. All electronic card reader access systems with which Verizon MA is familiar come with the ability to use the card for exit, called an "anti-passback" feature. If the authorized user does not use the card to check out, it invalidates the card for any future use until the system administrator can reset the card in the system. Such systems provide little additional security regarding who may enter a building. It is surprising that a CLEC advocates use of such systems, as the inadvertent failure of a CLEC technician to swipe his or her card upon exiting (*e.g.*, for lunch or to obtain a part from the truck) would temporarily prevent that technician's return to perform further service activities in the building.

Q. Please respond to Qwest's claims that it has replaced most key access with electronic access while Verizon MA has deployed such measures in only 15% of its central offices with allocated facilities (Qwest Testimony at 21).

A. Deployment of CRAS in Verizon MA's central offices has been based in part on the fact that physical collocation arrangements are generally located in secured and separate

space, rather than in space where other carriers' personnel also have access to Verizon MA's equipment. Verizon MA has generally found key access arrangements to be satisfactory under these conditions. Qwest has not provided the Department with any information concerning the design and configuration of collocation space in its offices, so a mere comparison of the percentage of central offices with CRAS systems has no meaning.

Q. Even so, please describe Verizon MA's current and planned deployment of CRAS at central offices.

A. Currently, CRAS is deployed in 34 central offices. Upgrades are underway in some of these offices and should be completed by the end of 2002. In addition, Verizon MA projects that it will deploy CRAS in 27 additional central offices by the end of 2002.

Q. AT&T disagrees with Verizon MA's assertion that breaches of security protocols by CLEC employees go unpunished because Verizon MA does not have the same recourse against CLEC violators as it does with its own employees or vendors. AT&T suggests that the consequences of improper actions by CLEC personnel can range from revoking an individual's access authorization to the pressing of criminal trespass charges (AT&T Testimony at 15). Please comment.

A. Verizon's personnel do work cooperatively with collocated carrier managers to resolve known security breach issues and building access violations or incidents involving misuse and improper use of IDs and access cards (see the response to information request AG

1-1). These measures are a useful part of a collocation security plan, but are not themselves sufficient.

VII. VERIZON MA'S PROPOSED COLLOCATION SECURITY PLAN IS NOT UNLAWFUL, ANTI-COMPETITIVE, OR DISCRIMINATORY

Q. Please address the claims of certain parties (*e.g.*, WorldCom Testimony at 3; Sprint Testimony at 4-5) that Verizon MA's proposals do not address security against terrorism but merely advance an anticompetitive agenda.

A. Contrary to the other parties' claims, Verizon MA is not using this inquiry as an opportunity to promote its own competitive interests. Verizon MA is responding to the Department's request for information and reasonable recommendations on measures that can be considered to improve security so as to protect the telecommunications network. As Verizon MA has shown above, its security proposal provides enhanced protection against intentional or inadvertent damage to essential parts of its network. Also as shown above, the parties' claims of increased costs, administrative burdens, and adverse effects upon their operations are greatly exaggerated. For example, Verizon MA's proposal that all physical collocation should be in separate, secured space is a continuation of current practice. In addition, as many commenters note (*e.g.*, Sprint Testimony at 4; WorldCom Testimony at 11; Qwest Testimony at 6), the networks of Verizon MA and CLECs are interconnected and interdependent;

increasing the security of Verizon MA's network enhances, rather than inhibits, the ability of CLECs to serve their customers.

Q. Please respond to AT&T's claim that Verizon's proposal "directly violates both the 1996 Telecommunications Act, as well as FCC rules implementing that law which required ILECs such as Verizon MA to provide physical collocation, except where precluded by space limitations or technical considerations" (AT&T testimony, page 18) and "is a far cry from what the FCC considers to be *reasonable* security measures" (AT&T Testimony at 20).

A, Verizon MA disagrees with AT&T's contentions. Security and operational considerations are reasonably a part of the technical feasibility equation. The FCC clearly recognized that security concerns warrants providing physical collocation by means of separate secured collocation areas or entrances. The only condition is that such arrangements not materially delay the collocated carrier's access to collocation or materially increase its costs of obtaining collocation over other means of providing for security of the central office where collocation is provided. Given that the Department has already ruled that physical collocation arrangements generally should be in separated, secured space, Verizon MA's proposals are appropriate.

Q. Is this also true for Verizon MA's proposal to designate certain critical central offices as available for virtual collocation only?

R. Yes. The Department may under the federal standards determine whether and to what extent security concerns constitute a technical feasibility limitation on physical collocation

in particular cases. Alternatively, the Department also has the discretion, as stated in its Order initiating this proceeding, to petition the FCC for a limited waiver of the rules if it determines that security considerations warrant the preclusion of physical collocation in these central offices.

Q. Is Verizon MA's proposal reasonable based on the FCC requirement regarding "legitimate security concerns", as cited by AT&T (AT&T Testimony at 25).

A. Yes it is. Verizon MA has demonstrated that there are legitimate security concerns when other carriers' personnel have unrestricted access to or through Verizon's equipment areas, where they have no legitimate reason to be. Indeed, Verizon MA's current practice and its proposed requirements regarding separate space are consistent with AT&T's current security policies.

Q. Please describe AT&T's security procedures.

A. AT&T enforces similar if not more stringent procedures in its Massachusetts central offices. Depending on the AT&T office, Verizon MA employees must have a valid ID and display it to the building guard, and may have to request access to locked areas from the guard and sign in to gain building entry during normal business hours. During non-business hours, Verizon employees must, depending on location, call either an out of state telephone number or an internal building number and wait for access, or wait for the next day for access. In at least two locations, access is only granted when, and if, an off-site AT&T employee arrives to admit the Verizon employee.

Q. Does AT&T place Verizon MA's equipment in separate space?

A. Verizon MA's equipment is usually required to be placed in cages or rooms with other carrier's equipment, that in either arrangement is physically separated and secured from AT&T's equipment area(s). In addition, Verizon's access to the caged arrangement or separate room, which is usually locked, requires either keypad or a card reader access that remotely displays on the guard's desk to access the cage or separate room in order for Verizon to access its equipment. In at least one location, the Verizon employee receives a "swipe" card that provides access and also operates the elevator.

Q. Can you give examples of other carriers' security measures?

A. NEON recently modified its procedures for access to its location in Worcester. Under the old arrangement, Verizon could obtain access 24 hours a day by contacting NEON from a communication panel located outside the door to NEON's facility and providing the technician's name and either Social Security number or company identification number. The new arrangement was established by NEON since September 11, 2001, and requires Verizon to provide 48 hours' notice to obtain escorted access to the facility.

Q. Does Verizon MA object to AT&T's or NEON's procedures?

A. No. These security measures are reasonable, and Verizon MA is simply seeking to implement similar measures for separation and securing other collocating carriers' equipment space in Verizon MA's central offices.

Q. Did any party demonstrate the competitive harm that they claim would result if Verizon MA's collocation security proposal was adopted?

A. No. Although parties made conclusory allegations that Verizon MA's proposals resulted in anti-competitive and discriminatory treatment, they have provided no cost data or other concrete evidence of harm, much less harm that outweighs the important security concerns at issue here.

Q. Please respond to Sprint's claim that Verizon MA's proposed security solutions are one-sided and apply only to CLECs and not to other carriers that collocate in a Verizon MA central office.

A. Verizon MA's proposed measures are intended to apply to all collocating carriers, not just CLECs.

Q. AT&T argues that in the event of a major service disaster, Verizon MA's lack of familiarity and training with virtually collocated CLEC equipment would cause it to work on its own equipment first and on virtually collocated CLEC equipment later (AT&T Testimony at 21-22). Do you agree?

A. No. Verizon MA employees would be familiar with and trained to maintain virtually collocated CLEC equipment. In addition we are obligated to restore Verizon's own and other carrier's service on a nondiscriminatory basis. Depending on the nature of the outage, this would include not only the virtual collocation equipment provided by the carrier but also the interconnected Verizon MA switching and transport facilities and unbundled network elements that are being accessed through the collocation arrangement.

.Q. Please respond to Qwest's claim that Verizon MA's proposal to require Qwest personnel applying for identification badges and access cards to authorize Verizon to perform background checks, while not requiring background checks of Verizon MA contractors, violates the nondiscrimination requirements under state and federal law. Please respond.

A. As noted in its response to Information Request AL-VZ 1-2, Verizon MA is in the process of working with its vendors to adopt a pre-screening process on a going-forward basis. Additionally, Verizon MA does not propose to conduct screening of any carrier's personnel or their contractors. Verizon's proposal is to have the carrier certify that it has conducted the requisite screenings and background checks.

Q. Do you agree that Verizon MA's proposed critical office limitation would result in stranded investment in the physical collocation areas abandoned by CLECs that would no longer be used, and have to be removed (AT&T Testimony at 26)?

A. No. As we explained earlier, the equipment would be reused and re-designated in place. It would continue to provide the same service as before the conversion.

Q. Do you agree with AT&T (pp. 26-27) that the minimal amount of additional security provided by facility separation would not be worth the man-hours, costs, and customer disruption associated with such conversions?

A. No. The additional level of security gained would not be minimal and would not be unlike that which AT&T's procedures provide. There would be no disruptions of customer service because there would be no physical relocation of collocated

equipment based on the existing central office configurations, and conversion of physical to virtual collocation would be in-place conversions.

Q. Please address the comments by Qwest and others that the Department should await establishment of national guidelines by governmental or national industry groups.

A. While these issues are nationwide in scope, the Department should ensure that sufficient security measures are in place to address concerns in Massachusetts. It is appropriate for the Department to proceed with its initiative rather than risk further delay waiting for developments on the national front. The Department, if needed, always has the opportunity to revisit any actions taken in this proceeding, if developments at the national level indicate that it would be appropriate to do so.

VIII. CONCLUSION

Q. Please provide a summary of your surrebuttal testimony.

A. The other parties have either misconstrued or misrepresented Verizon MA's proposals. Contrary to their claims, none of Verizon MA's proposals adversely affect competition. Rather, Verizon MA's collocation security proposal properly balances competitors' need for access to Verizon MA's central offices and the public's need for additional security measures to protect those central offices and preserve the telecommunication infrastructure.

Q. Does that conclude your testimony?

A. Yes.