COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

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

INITIAL BRIEF OF VERIZON MASSACHUSETTS

In this Initial Brief, Verizon Massachusetts ("Verizon MA") shows that its collocation security proposal is a reasonable and effective means of proactively protecting Verizon MA's central office ("CO") locations and remote terminal equipment enclosures ("RTEE") in Massachusetts and reducing the potential risk of harm to the telecommunications network infrastructure. The thrust of Verizon MA's proposal is to reduce the risk by limiting access or "foot traffic" in its Massachusetts COs. While no security measures are foolproof, Verizon MA's proposal is a reasonable and prudent approach, particularly in light of the events of September 11, 2001.

Recently, Verizon MA has taken steps to enhance its current security procedures by strengthening employee and non-employee background checks and expanding the deployment of electronic access entry systems to COs. While such action may be a deterrent, it will not *prevent* damage to the critical telecommunications infrastructure that can occur either accidentally or intentionally when carriers have unrestricted access to COs in a physically collocated environment.

As explained below, Verizon MA's collocation security proposal would maintain the current policy of establishing separate space, as well as separate entrances and/or secured pathways, for physical collocation. In addition, the proposal would establish virtual collocation as the *exclusive* form of collocation under certain limited conditions. Exh. VZ MA 2, at 8-10. Those conditions are as follows: (1) when no separate and secured space is available in the CO; (2) in remote terminal ("RT") locations; and (3) in "critical" COs, as determined by the Department. Tr. 361. By limiting access under the circumstances, Verizon MA would minimize significantly the likelihood of considerable network harm resulting from deliberate or unintentional damage to Verizon MA's equipment and facilities in those vulnerable locations. Implementation of such security measures is also consistent with the letter and the spirit of the Telecommunications Act of 1996 (the "Act') and the Federal Communications Commission's ("FCC") decisions enforcing the Act.

Contrary to some parties' claims,[1] Verizon MA's collocation security proposal is not anti-competitive, and would not unduly interfere with providing carriers reasonable access to their collocated facilities. In fact, the additional security will benefit carriers by enhancing the security and reliability of their networks, which are interconnected with Verizon's. In addition, Verizon MA's proposed plan would apply equally to all collocators,[2] and would not impede competition in any way. Tr. 62, 112, 139.

---

[1] For purposes of this Brief, Verizon MA refers to the following carrier-intervenors collectively as the "parties:" Allegiance Telecom, Inc. ("Allegiance"), AT&T Communications of New England ("AT&T"), Conversent Communications of MA, LLC ("Conversent"), Covad Communications Company ("Covad"), Qwest Communications Corporation ("Qwest"), Sprint Communications Company ("Sprint"), WorldCom, Inc. ("WCOM"), and XO Massachusetts, Inc. ("XO"). The non-carrier intervenors in this proceeding are the Office of the Attorney General ("Attorney General" or "AG") and the International Brotherhood of Electrical Workers ("IBEW").

[2] Verizon MA would apply its proposed security measures to all collocators, regardless of whether

Accordingly, the Department should reject the other parties' unsubstantiated claims and adopt Verizon MA's collocation security proposal. That proposal provides the necessary *preventive* measures to better protect Verizon MA's investments, preserve its and the other carriers' networks, and maintain its ability to provide continuous and reliable service for its end user and carrier customers by ensuring a more secure collocated environment.

I. INTRODUCTION AND SUMMARY

The Department opened this investigation in its January 24, 2002, Order ("*Order*"), to examine Verizon MA's existing collocation security policies access by personnel of other carriers to Verizon's COs and other facilities. *Order*, at 1. The Department's intent was to assess whether those security measures, which were established in accordance with the Department's findings in D.T.E. 98-57, Phase I,[3] would adequately protect the telecommunications network and facilities in light of heightened security concerns following the September 11th terrorist attacks in New York City and Washington, D.C., or whether *additional* collocation security measures are warranted. *Id.* at 1.

The Department raised the following issues for review in this investigation: (1) the extent and nature of appropriate access by personnel of other carriers to Verizon's central offices and other facilities [*e.g.*, remote terminals] for accessing collocation sites;

---

they operate as interexchange carriers ("IXCs"), competitive access providers ("CAPs"), competitive local exchange carriers ("CLECs"), alternative local transport providers ("ALTS"), or commercial mobile radio service ("CMRS") providers. Exh. Sprint-VZ 2-21. For purposes of this Brief, they are referred to collectively as "carriers."

[3] *See* D.T.E. 98-57, Phase I, *Order*, at 24-39, 59-62 (March 24, 2000); D.T.E. 98-57, Phase I, *Reconsideration Order*, at 6-16, 66 (September 7, 2000); D.T.E. 98-57, Phase I, *Phase I-B Order*, at 16-20 (May 24, 2001).

(2) whether cageless collocation arrangements remain an acceptable security risk; (3) the adequacy of security measures implemented in Verizon's central offices and other facilities, focusing on preventive, rather than "after-the-fact," measures; and (4) any other related security issues. *Id.* at 7. The Department also stated that it will determine whether Verizon's security policies meet the statutory standard for "just, reasonable, safe, adequate and proper regulations and practices." Mass. General Laws, c. 159, §16. *Order,* at 7.

Consistent with actions taken by other entities (*e.g.*, airports, government facilities, etc.) since September 11th, the Department recognizes that "access" to COs should be the primary focus of strengthening collocation security procedures.[4] Exh. Qwest-VZ 1-3. Verizon MA's current requirements for providing other carriers "access" to collocation space[5] were established by the Department and the FCC prior to September 11th. Given the critical importance of telecommunications and the heightened concern over security, it is critical to re-examine those requirements and the potential security risks associated with permitting carriers' unrestricted access to or through Verizon MA's equipment areas. Exh. VZ MA 2, at 2.

As the Department's *Order* suggests, Verizon MA's collocation security measures for its Massachusetts COs should be strengthened "to safeguard the telecommunications

---

[4] Verizon MA believes that it is *not* the Department's intent to examine ways to physically fortify COs to withstand crashing planes or bombs, or equip COs with anti-aircraft defense systems to fend off terrorist attacks. Exh. Qwest-VZ 1-3; Exh. VZ MA 2, at 3. After all, it was not only crashing a plane, but the series of events leading up to that act (*e.g.*, lax enforcement of immigration policies, access to flight school lessons by those on "high security watch" lists, failure to adequately screen airplane passengers for possession of weapons, etc.) that enabled the events of September 11th to occur. Exh. Qwest-VZ 1-3.

[5] Those 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. Exh.

networks from tampering" and "ensure that reliable service to competing telecommunications service providers, businesses, and residents of the Commonwealth is not unreasonably at risk" post September 11th. *Id.* at 2. The increased potential for network harm resulting from increased foot traffic in Verizon MA's physically collocated facilities[6] necessitates a higher *baseline* level of security in all collocated COs post September 11th, as Verizon MA recommends. Tr. 24. That conclusion is supported by Verizon's experience with security breaches in Massachusetts and elsewhere. Exh. AG-VZ 1.

Deploying such security devices as cameras, electronic card readers, or badges with computerized tracking systems may enable the detection of security breaches "after the fact," and may even *deter* them in some cases. Exh. VZ MA 1, at 2. However, such equipment alone does not enable Verizon MA to deter or prevent inadvertent or intentional incidents that could harm the network and disrupt service for the millions of end user and carrier customers served by those facilities. Exh. VZ MA 2, at 3. As discussed below, Verizon MA needs to be able to *restrict* access to unsecured areas within the CO and, in some cases, to the entire CO and RT. Exh. VZ MA 1, at 3.

Although pro-active security measures (*e.g.*, separate space and separate entrances and/or pathways) cannot totally eliminate security risks, they can substantially minimize them. Exh. VZ MA 2, at 3. This will enable Verizon MA to better protect and preserve

---

VZ MA 2 at 2.

6 In Massachusetts alone, there are 46 CLECs who currently have 948 physical collocation arrangements and 5 virtual collocation arrangements in 169 Verizon MA COs. Exh. VZ MA 1, at 40; Tr. 739. The sheer number of collocators – and the vast number of technicians, vendors, supervisors, contractors, and other personnel that support those collocators – substantially increase the traffic through Verizon MA's COs. This, in turn, vastly increases the *probability* of accidents, mistakes, and outright wrongdoing and, therefore, the exposure to financial harm and damage to Verizon MA's network. Exh. VZ MA 1, at 22-23, 27.

the network in a physically collocated environment so that Verizon MA and other service providers can maintain uninterrupted service for their end-user customers, which include state and federal government installations and businesses that are critical to the public welfare. Without such proactive security measures, Verizon's network, as well as the facilities, equipment, and capabilities of collocated carriers, remain exposed to an increased risk of harm. Therefore, the Department should find that Verizon MA's collocation security proposal appropriately addresses the legitimate security concerns raised in its *Order*, and reflects "just, reasonable, safe, adequate and proper regulations and practices" under Section 16 of Chapter 159 of the Massachusetts General Laws.

II. DESCRIPTION OF VERIZON MA'S COLLOCATION SECURITY PROPOSAL

The basic tenet of Verizon MA's collocation security proposal is to reduce the potential for network harm by minimizing the opportunity for contact with Verizon's network infrastructure by collocators' employees and contractors. As stated by Verizon's Security experts, "less [foot] traffic in the central office equates to less risk." Tr. 60, 63, 137. In other words, by limiting access to the CO, there is "less possibility of either a service outage or theft, or some other issue that requires a security response." Tr. 60. This is particularly true post-September 11th.

To address those security concerns,[7] Verizon MA recommends that the Department adopt the following *pro-active* collocation security measures:

[7] From a pure security standpoint, the most effective means of ensuring network safety and reliability is to eliminate physical collocation entirely in all Verizon MA COs, converting existing physical collocation arrangements to virtual and requiring that all future collocation arrangements be virtual only. Tr. 719; *see* Tr. 586-87 (Mr. Adragna of Qwest). However, Verizon MA recognizes that this is not a practical solution from a legal and regulatory perspective at this time. Exh. VZ MA 1, at 3-4.

1. the establishment of separate space with separate entrances and/or pathways for all forms of physical collocation (*i.e.*, caged and cageless) to secure and segregate collocators' equipment from Verizon MA's equipment and no commingling of collocators' equipment in the same rooms as Verizon MA's equipment without some reasonable means of physical separation (*e.g.*, partitioning) and secured access;

2. the relocation of existing *unsecured* cageless collocation arrangements to a secured and segregated area of the CO or the conversion of such arrangements to virtual collocation where secured CO space is unavailable;

3. the provision of reasonable access to shared facilities (*e.g.*, temporary staging areas, elevators, loading docks, restrooms, etc.) that are located outside the secured and segregated collocators' space either by partitioning Verizon MA's equipment, if feasible, or through the use of escorts at the collocated carrier's expense;

4. the requirement to provide virtual collocation and/or escorts at physically collocated remote terminal ("RT") sites; and

5. the development of more stringent measures in critical, "high" security risk COs, *i.e.*, classify such COs as "virtual collocation only" sites.

Exh. VZ MA 1, at 4. Other initiatives undertaken by Verizon MA to enhance security include: (1) the expansion of existing criminal background checks and drug screening tests for its own employees and contractors, and the requirement that collocators conduct and certify comparable background checks for their employees and contractors before Verizon issues identification ("ID") badges; and (2) the expanded deployment of electronic surveillance, *i.e.*, card reader access systems ("CRAS"), in Massachusetts COs. Exh. VZ MA 1, at 5; Tr. 96, 101, 110, 128-29; Exh. Qwest-VZ 1-20; Exh. Qwest-VZ 1-21.

While most of the above proposed security measures reflect a continuation of Verizon MA's current collocation policies and procedures (*e.g.*, separate and segregated space, separate entrances and/or secured pathways; reasonable access to common areas, etc.), there are some important differences. Exh. AL-VZ 2-2.

First, under current regulatory rules, Verizon MA may not relocate or convert unsecured cageless collocation arrangements. Tr. 363. Verizon MA strives to establish separate and secured space - as well as separate entrances and/or secured pathways - for *all* physical collocation (caged and cageless) arrangements in Massachusetts.[8] However, even if *separate* physical collocation space is unavailable due to space constraints in a particular CO, Verizon MA is required to provide CCOE, if requested. Exh. VZ MA 1, at 32-33; Tr. 363. In Massachusetts, there is one existing CCOE arrangement in the Hopkinton CO that is located in an *unsecured* area where Verizon MA's equipment is already placed and cannot be segregated.[9] Tr. 47-48; Exh. AL-VZ 1-9; Exh. AL-VZ 1-21; Exh. Conversent-VZ 1-20.

---

[8] Tr. 266-67. The typical forms of physical collocation available in most Massachusetts COs include: (1) traditional "caged" physical collocation, (2) secured collocation open environment ("SCOPE"); and (3) cageless collocation open environment ("CCOE"). Exh. VZ MA 1, at 9. Verizon MA also offers virtual collocation, adjacent collocation; shared collocation, microwave collocation, and collocation at remote terminal equipment enclosures ("CRTEE"). *Id*. Currently, Verizon MA provides 536 traditional "caged" physical collocation arrangements, 385 SCOPE, 27 CCOE, five virtual collocation arrangements, and one shared collocation arrangement located in a total of 169 COs in Massachusetts. *Id*.; Tr. 739. To date, Verizon MA has not provisioned any CRTEE, adjacent or microwave collocation arrangements. However, the Company is currently processing one customer's physical collocation application for microwave entrance facilities in Massachusetts. Exh. VZ MA 1, at 9 n.5.

[9] Because the Hopkinton CO is extremely small, the building configuration cannot accommodate physically separating the carrier's equipment from Verizon MA's facilities. Therefore, that one CCOE arrangement cannot be relocated due to a lack of secured and separate space in the CO, and would be converted to a virtual collocation under Verizon MA's collocation security proposal. Exh. AL-VZ 1-3. This would have minimal impact on collocators because only one carrier is affected. Exh. AL-VZ 1-21. That carrier would incur no additional costs to convert the existing arrangement "in-place" to virtual collocation in accordance with Verizon's applicable tariffs. *See* Exh. Sprint-VZ 2-11, *citing* D.T.E. MA Tariff No. 17, Part E, Section 2.2.8; Tariff F.C.C. No. 11, Section 28.1.5(C).

This intermingling of a carrier's cageless arrangement with Verizon MA's equipment raises serious security concerns, as described below. Exh. VZ MA 1, at 33. Therefore, Verizon MA seeks the ability to prevent such configurations in the future by requiring virtual collocation if secured segregated space cannot technically be made available for physical collocation in a CO.[10] Exh. VZ MA 2, at 18; Tr. 363. This would enable Verizon MA to limit future cageless collocation arrangements to only those COs where Verizon MA has or can provide secured segregated space. Tr. 144, 363. Verizon MA also seeks Department approval to convert "in-place" to virtual collocation the one existing unsecured cageless arrangement in Massachusetts. Exh. VZ MA 1, at 33-34; Exh. VZ MA 2, at 18; Tr. 144-45.

Second, Verizon MA proposes that it be permitted to require virtual collocation in RTs. Exh. VZ MA 1, at 38. Because of the small size and structure of RTs, this is the only feasible way of addressing the unique security problems raised by RT collocation and protecting Verizon MA's network facilities and equipment. Exh. VZ MA 1, at 36-38; Exh. VZ MA 2, at 13-14. Although no RT collocation arrangements currently exist in Massachusetts, Verizon MA seeks Department approval of its proposal in the event that such collocation is requested by a carrier in the future. Exh. VZ MA 1, at 35-36; Exh. VZ Ma 2, at 12.

Third, Verizon MA recommends that the Department adopt Verizon MA's proposal for "critical offices" and implement a *process* to identify those COs that would

[10] Currently, Verizon MA files an exemption with the Department when a CO is closed to physical collocation, and converts the CO to virtual collocation only. Exh. Qwest-VZ 1-30. If the Department approves Verizon MA's proposal to restrict CCOE to secured space, then the Company would file an exemption restricting a CO to virtual collocation when physical collocation (including CCOE) is only available in *unsecured* areas of the CO. Exh. VZ MA 2, at 10.

warrant this heightened level of security. Exh. VZ MA 2, at 14-17; Tr. 85. Because a security violation at "critical" CO poses potentially more serious and widespread harm to the telecommunications network and public safety, only virtual collocation should be provided at those COs, even if secured and separate space for physical collocation is otherwise available. Exh. VZ MA 1, at 38; Exh. AL-VZ 2-2. The designation of critical offices would be based on specific criteria to be determined by the Department. Exh. VZ MA 1, at 38; Tr. 24, 232. The Department may use the various factors described by Verizon MA as the basis for developing a framework to define that criteria.[11] Exh. VZ MA 1, at 39-40; Exh. VZ MA 2, at 14-17; Exh. XO-VZ 1-4; Exh. AL-VZ 2-2.

Likewise, Verizon MA requests that any existing physical collocation arrangements in those designated critical COs be converted to virtual collocation arrangements. Exh. VZ MA 1, at 39-40. Where feasible, physical collocation would be converted to virtual "in place," thereby minimizing any added security costs borne by the collocators.[12] Exh. VZ MA 1, at 40.

A. Applicable Law

In accordance with FCC rules, Verizon MA "must allow collocating parties to access their collocated equipment 24 hours a day, seven days a week, without requiring

---

[11] The key factors to consider in determining the critical nature of a central office may include: (1) the type of switch or signaling elements housed in a CO; (2) the presence of critical customers (*e.g.*, major airport, military installation, government agencies, and/or nuclear power plant) served by a CO; and (3) the number of access lines and special services circuits served by a CO. Exh. VZ MA 1, at 39; Tr. 82-83; Exh. VZ MA 2, at 15. For example, a CO may be more critical if it houses a tandem switch, an emergency 911 ("E911") tandem switch, and/or Signal Transfer Point ("STP") equipment that are the "lifeline" to numerous subtending switches throughout Massachusetts. Exh. VZ MA 1, at 39.

[12] Since these would be in-place administrative conversions, they would be treated like a rearrangement or relocation of a physical collocation enclosure in accordance with Verizon MA's applicable state and federal tariffs. Exh. Sprint-VZ 2-11, *citing* D.T.E. MA Tariff No. 17, Part E, Section 2.2.8; Tariff F.C.C. No. 11, Section 28.1.5(C).

either a security escort of any kind or delaying a competitor's employees' entry" to the CO premises. 47 C.F.R. § 51.323(i); Exh. VZ MA 1, at 33. Verizon MA must also allow collocators "reasonable access to basic facilities" (*e.g.*, temporary staging areas, elevators, loading docks, restrooms, etc.) while at the Company's premises.[13]

Verizon MA may require reasonable security arrangements to protect its own equipment and ensure network reliability in a collocated environment. *Advanced Services Order*, ¶ 46; Tr. 220-21. The security arrangements imposed, however, may only be as stringent as those Verizon applies to itself or its authorized vendors. Exh. VZ MA 1, at 12.

Reasonable security measures[14] that Verizon MA may adopt for its collocation arrangements are set forth in 47 C.F.R. §51.323(i). They include:

> (1) installing security cameras or monitoring systems;
>
> (2) requiring CLEC personnel's use of badges with computerized tracking systems;
>
> (3) requiring CLEC personnel to undergo the same or equivalent level of security training as Verizon's own employees or authorized vendors, provided that the CLEC is not required to receive such training solely from Verizon;
>
> (4) restricting physical collocation space to space that is physically separated from space housing Verizon's equipment;[15] and

---

13 *See Deployment of Wireline Services Offering Advanced Telecommunications Capability*, First Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 98-147, 14 FCC Rcd 4761, at ¶ 49 (March 31, 1999) ("*Advanced Services Order*").

14 *See Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Fourth Report and Order, CC Docket No. 98-147, FCC 01-204 (rel. Aug. 8, 2001) ("*Collocation Remand Order*"), on remand from the U.S. Court of Appeals' decision in *GTE Service Corporation v. FCC*, 205 F.3d 416 (D.C. Cir. 2000) ("*GTE Service Corporation*"). The FCC has found that incumbent local exchange carriers ("ILECs") should be permitted "to recover the costs of implementing these security measures from collocating carriers in a reasonable manner." *See Advanced Services Order*, ¶ 48.

(5) requiring access through a central or separate entrance provided that Verizon affiliates and subsidiaries have the same requirement.[16]

In providing reasonable security arrangements, Verizon MA may require carriers to pay only for the least expensive, effective security option that is viable for the physical collocation space assigned. 47 C.F.R. §51.323(i).

The FCC has also recognized that security and network reliability are valid factors that must be considered when evaluating whether physical collocation is technically feasible under the Act.[17] Tr. 239. Section 251(c)(6) states that virtual collocation is provided "where physical collocation is not practical for technical reasons or because of space limitations" in a particular CO, and is also available as an option for a CLEC in *any* CO. 47 U.S.C. § 251(c)(6). In its *Local Competition Order*, the FCC explicitly concluded that:

---

15 This type of security measure is subject to the following conditions: (i) either legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant such separation; (ii) any physical collocation space assigned to an affiliate or subsidiary of the incumbent LEC is separated from space housing the incumbent LEC's equipment; (iii) the separated space will be available in the same time frame as, or a shorter time frame than, non-separated space; (iv) the cost of the separated space to the requesting carrier will not be materially higher than the cost of non-separated space; and (v) the separated space is comparable, from a technical and engineering standpoint, to non-separated space. 47 C.F.R. §51.323(i)(4); Tr. 241-47.

16 The following conditions must be met to apply this security measure: (i) construction of a separate entrance is technically feasible; (ii) either legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant such separation; (iii) construction of a separate entrance will not artificially delay collocation provisioning; and (iv) construction of a separate entrance will not materially increase the requesting carrier's costs. 47 C.F.R. §51.323(i)(6).

17 *See e.g., In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*, CC Docket No. 96-98, FCC 96-325, *First Order and Report* (rel. August 1996), ¶ 203 ("*Local Competition Order*"); *see e.g.* CC Docket Nos. 01-338, 96-98, 98-147, FCC 01-361, *Notice of Proposed Rulemaking* (rel. December 20, 2001), ¶ 33. In that Order, the FCC asked commenters "to identify any additional factors not raised previously for consideration in our unbundling analysis that would further statutory goals. For example, should issues of public safety, national security, or network integrity be explicitly considered in our implementation of section 251?" *Id*.

> [L]egitimate threats to network reliability and security must be considered in evaluating the technical feasibility of interconnection or access to incumbent LEC networks. Negative network reliability effects are necessarily contrary to a finding of technical feasibility. Each carrier must be able to retain responsibility for the management, control and performance of its own network. Thus, with regard to network reliability and security, to justify a refusal to provide interconnection or access at a point requested by another carrier, incumbent LECS must prove to the state commission, with clear and convincing evidence, that specific and significant adverse impacts would result from the requested interconnection or access.

Local Competition Order, ¶ 203. In light of the FCC's findings, the Department has the authority to determine whether physical collocation in a given CO is technically feasible based on legitimate security concerns, or whether virtual collocation would be required because physical collocation is not practicable. Tr. 249; Exh. Sprint-VZ 2-19.

Likewise, virtual collocation may be required for RT collocation based on security reasons. The FCC is currently reviewing the appropriate security measures for RT arrangements in connection with its *Collocation Remand Order*, and has specifically sought comments on whether virtual collocation constitutes an acceptable replacement for physical collocation at RTs.[18] The FCC has not yet completed this phase of its proposed rulemaking or established final rules on this issue. However, current FCC rules do not prohibit this approach.[19] Exh. VZ MA 2, at 13-14.

---

[18] *In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*, CC Docket Nos. 98-147 & 96-98, FCC 00-297, *Order on Reconsideration and Further Notice of Proposed Rulemaking* (rel. August 2000), ¶¶ 40, 44, 104 ("*FCC Reconsideration Order*").

[19] Verizon MA disagrees with the Department's conclusion that the existing FCC rules prohibit escorts for RT collocation. D.T.E. 98-57, *Phase I-B Order*, at 19. The issue of requiring escorted access to controlled environmental vaults ("CEV") and huts is also currently under review at the FCC. *FCC Reconsideration Order*, ¶ 104.

Finally, the Department's findings on collocation security measures in its D.T.E. 98-57, Phase I, Orders are generally consistent with the above FCC's requirements[20] under 47 C.F.R.. Exh. VZ MA 1, at 14. Like the FCC, the Department recognized the need to limit carrier access within the CO and enable Verizon MA to preserve and protect the network infrastructure.[21]

III. ARGUMENT

Verizon MA's collocation security proposal provides an appropriate *baseline* level of network security for collocated COs and RTs in Massachusetts by restricting "foot traffic" or access by collocators in areas where Verizon MA's facilities and equipment are located. Tr. 24, 200. This is reasonable and necessary because of the inherent design and network functionality of those structures - and the potential to target telecommunications facilities, which are generally considered a high security risk.[22] Exh. VZ MA 2, at 5-6; Exh. AL-VZ 1-25.

---

[20] This includes the use of security cameras, electronic card readers, and badge tracking systems. *Order*, at 27. Other security measures permitted by the Department include: (1) a 30-minute prior notification by the CLEC to Verizon before dispatching a technician is sufficient for both manned and unmanned central offices; and (2) the designation of a specific (even separate) entrance for CLEC use during work stoppages. *Id*. at 32, 39. The Department further clarified that it does not intend to prohibit Verizon from deploying an efficient mix of security measures within a CO, but rather to prevent the deployment of duplicative security measures that would increase the costs of collocation without providing a necessary security benefit. *Reconsideration Order*, at 15.

[21] In clarifying the issue of carrier access beyond their collocation arrangement, the Department stated that Verizon MA may prohibit a carrier from access to any area within the CO where the carrier does not have any collocated equipment located. *Reconsideration Order*, at 15. Finally, the Department issued a stay on its earlier directives regarding the construction of separate collocation rooms, the commingling of equipment, and conversions from virtual to cageless collocation, pending a final decision by the FCC on those issues. *Reconsideration Order*, at 15.

[22] While no one can predict with certainty where acts of sabotage will occur, national security experts believe that telecommunications infrastructure facilities as well as other infrastructure facilities are potential targets. Exh. VZ MA 2, at 5-6. As revealed by Attorney General John Ashcroft, the FBI has issued warnings through the National Threat Warning System to companies that own and operate systems, including telecommunications infrastructure systems, to prepare for a new wave of attacks. *Id*. at 5-6. John Tritak, Director of the U.S. Commerce Department's Critical Infrastructure Assurance Office, also said in a statement to the Senate Government Affairs Committee on October 4, 2001, "[t]hat the loss of telecommunications services can impede

Parties have mischaracterized Verizon's collocation security proposal in a number of ways. Among their principal claims are that Verizon MA's proposal represents a radical change from current practices and that Verizon MA is acting anticompetitively by attempting to burden CLECs with unnecessary requirements and costs. Exh. VZ MA 2, at 7. Some parties even suggest that Verizon MA's proposal is an attempt to eliminate physical collocation entirely in Massachusetts. Exh. VZ MA 2, at 17; Exh. AL 1, at 8. Those allegations are false.

Verizon MA's proposal would have minimal impact on existing collocators because it is essentially a continuation of the Company's present collocation security policies, except for the "critical office" component.[23] Tr. 47-48. Contrary to the parties' claims, Verizon MA's proposal is also consistent with applicable regulatory and legal requirements, and is not anti-competitive, discriminatory or unlawful.

A. Limiting Access in Verizon MA's COs and RTs Is Necessary to Protect Both Verizon's and Collocators' Networks.

Both end-user and carrier customers depend on the reliability of Verizon MA's telecommunications network to provide the backbone platform for data, voice, and long distance services. Exh. VZ MA 1, at 25; Exh. AL 1, at 2; Exh. Covad 1, at 7; ; Tr. 412-13. The CO is an integral part of Verizon MA's network infrastructure because it is the "hub"[24] where network access lines and interoffice facilities are combined to connect with

---

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." *Id*. at 6.

23 Only one carrier would be affected by the requirement to relocate or convert existing unsecured cageless arrangement to virtual collocation. No carrier would be affected by the RT virtual collocation requirement because no RT collocation currently exists in Massachusetts.

24 Generally, CO buildings contain, *inter alia*, switching equipment, transmission circuit equipment, common channel signaling systems, distribution frames and cross-connections systems, power

other facilities to provide telecommunications services to residence and business customers, including governmental, financial and public safety organizations. Exh. VZ MA 1, at 24 and Att. 3. It is also the point where carrier customers interconnect their networks to Verizon or subscribe to the Company's wholesale or retail services. *Id*.

Moreover, some COs contain tandem switches, signal transfer points ("STP"), or E911 switches and adjunct equipment, each of which is critical to the network as they are used to complete interoffice and emergency calls. *Id*. at 26. Based on current technology and network configurations and the critical and highly sensitive nature of the equipment located in Verizon MA's COs, any inadvertent or intentional damage[25] in a given CO may impair multiple end offices with potentially significant service-affecting consequences, including but not limited to the interruption of public safety or emergency services. *Id*. at 24-25. In addition, the degree of interconnection and interdependence among Verizon MA's and other carriers' networks means that damage to Verizon's network can have substantial impact on those carriers' operations as well. Tr. 412-13, 415.

At the time that COs were originally built, they were designed to make efficient use of space and ensure that all of the equipment interconnected and functioned properly.[26] Exh. VZ MA 1, at 25. Likewise, the COs evolved over time, with equipment

---

plant, operating support systems, etc. Exh. VZ MA 1, at Att. 3; Exh. Sprint-VZ 2-4.

25 Not only is inadvertent or intentional damage to the CO's operational and electronic equipment a concern, but also damage to its power plant and environmental support infrastructure (*e.g*., water supply, heating, ventilation, and air conditioning system, etc.) must be prevented. Exh. VZ MA 1, at 26 n.22.

26 For example, equipment with similar functions is grouped together; room for growth is planned for equipment, such as switches and frames, that must be contiguous; certain equipment (*e.g*., power plant, circuit switches, interoffice and toll transmission equipment) may be segregated for technical and safety reasons; and infrastructure (*e.g*., power, heating, ventilation, air conditioning,

being placed where it made the most technical sense. COs were not, however, designed to accommodate or house equipment used by multiple carriers. For that reason, the CO building structure itself (*i.e.*, the exterior walls and doors of the premises) was the primary security measure to keep unauthorized individuals out.

With the advent of physical collocation, circumstances changed. The equipment of multiple carriers is now placed in Verizon MA's COs, and many more individuals are allowed access to Verizon MA's facilities. Exh. VZ MA 1, at 41. The greater influx of "foot traffic" dramatically increases the security risks to the network infrastructure and directly affects the type of security measures that can and must be imposed.

Although the presence of all types of physical collocation[27] inherently compromises Verizon MA's ability to protect its network from *within* the CO. This is particularly true of cageless or CCOE arrangements which are not required to be placed in secured areas of the CO.[28]

Based on the design of COs, placing locked cabinets around Verizon MA's equipment and network is neither technically or operationally feasible – nor an

---

etc.) is designed to support each component. In addition, switches and transmission equipment are on different ground planes (*i.e.*, isolated versus integrated) and cannot be commingled for safety and personnel reasons. Exh. VZ MA 1, at 25 n.20.

[27] The traditional "caged" physical collocation arrangement allows a carrier to place its equipment in a wire mesh enclosure or cage – available in varying standard sizes (*e.g.*, 25, 100 or 300 square feet) – within a segregated and secured, environmentally conditioned area of Verizon MA's CO. By contrast, SCOPE and CCOE are forms of physical collocation that allow the placement of a collocator's equipment in single bay (or rack) increments in Verizon MA's CO *without* requiring an individual cage or wire mesh enclosure. Tr. 143.

[28] While SCOPE arrangements are placed in the *same* segregated and secured, environmentally conditioned area used for traditional "caged" physical collocation, CCOE arrangements may not require the construction of a separate collocation area, *e.g.*, a separate room or isolated space segregated from Verizon MA's own network equipment, due to space limitations. Exh. VZ MA 1, at 10; Tr. 144; 47 C.F.R. § 51.323.

economically viable option.[29] Exh. VZ MA 1, at 26, 33. In addition, even if this were technically feasible, it would not be practicable because of the amount of available space in most Verizon MA COs. Exh. VZ MA 1, at 33. Accordingly, because Verizon MA is no longer the only carrier occupying the CO in a collocated environment, additional security measures are required for Verizon MA to protect its facilities and equpment.[30]

Like COs, RTs were not built to accommodate multiple carriers in a physically collocated environment. Exh. VZ MA 1, at 25; Exh. VZ MA 2, at 12. Rather, RTs were traditionally designed to protect the equipment from *within*, meaning that the facilities were locked and only authorized Company employees were permitted access to those sites. Exh. VZ MA 2, at 12-13. Because RTs house much of the same costly and delicate transmission and multiplexing equipment housed in a CO, they present the same opportunities for service disruption, equipment tampering and theft as COs. However, securing RTs is even more problematic because of their extremely small size and their remote location. Exh. VZ MA 1, at 36.

---

29 Verizon MA is not able to make space for such cabinets without moving equipment or reconstructing the entire heating, ventilation, and air conditioning system in its COs. Exh. VZ MA 1, at 33. Verizon MA must be allowed to protect its own equipment without having to resort to such massive reconstruction and reengineering. If new COs were built today, Verizon MA could design them with *interior* security in mind, and for example, place all of its sensitive equipment on one floor, and leave other parts of the CO with empty space for collocators. Verizon MA could also ensure that all the empty space in the CO was near a door that could be adequately secured. Exh. VZ MA 1, at 25 n.21.

30 By contrast, carriers have alternative security measures that are not available to Verizon MA because the building was previously Verizon's "secure envelope." For example, carriers can safeguard their equipment in locked physical cages with wire mesh enclosures and/or tops. Exh. VZ MA 1, at 32. They may also elect to install locking cabinets or covers for their equipment in caged or cageless collocation arrangements. *Id.*; Exh. Conversent-VZ 1-4. Within their collocation space, carriers have the option of installing their own overt or covert video surveillance and monitoring systems (*e.g.*, alarms, motion detectin security video), provided that the images recorded or transmitted are limited to the specific carrier's equipment or operating area, and do not include images of Verizon's or other carrier's areas or equipment. Exh. Conversent-VZ 1-8; Exh. Conversent-VZ 1-3. Similar security arrangements for Verizon MA's equipment would not be possible if separate space was not required and intermingling of equipment was permitted. Exh. VZ MA 1, at 32.

Verizon MA uses three basic forms of RT enclosures for digital loop carrier circuit equipment that is located remotely from the CO. 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. Exh. VZ MA 1, at Att. 3; Exh. VZ MA 2, at 12. CEVs and huts often are sized so that a single technician can enter and gain access to equipment and wiring in the limited space available. Exh. VZ MA 1, at 36. A technician gains access to cabinet-enclosed equipment and wiring from outside the structure through a hinged door opening. Exh. VZ MA 2, at 12.

Unlike a CO, RTs cannot be retrofitted or rearranged to accommodate the physical collocation of another carrier's equipment. Exh. VZ MA 2, at 12. The size of RTs make partitioning or securing Verizon MA's equipment inside a locked enclosure within the small RT virtually impossible. This is because of the additional space such an enclosure would occupy and the lack of excess space in the confined RT structure. Exh. VZ MA 1, at 37.

Likewise, because of the limited space in RTs, network facilities are more closely located with other facilities. Exh. VZ MA 1, at 36. As a result, the likelihood of service-affecting consequences is even greater in RTs than in COs. *Id*. Inadvertent or improper actions within the tightly engineered and confined space of RT can cause service disruptions for customers served through RTs just as if the damage originated in the CO. *Id*.

In conclusion, because of the design and structure of COs and RTs, the greater influx of "foot traffic" caused by physical collocation dramatically increases the potential risks to Verizon MA's network infrastructure. To address those legitimate security concerns,[31] the Department should enable Verizon MA "to secure its equipment in a secure envelope" by permitting the Company to restrict access within the COs and RTs and, under certain circumstances, limit to virtual collocation only. Tr. 219. This would reduce the risk of network harm and the far-reaching effects of a network outage on Verizon MA and the end-user and carrier customers served by those facilities. Exh. VZ MA 1, at 26.

B. The Incidence of Security Breaches in Massachusetts and Other Jurisdictions Justifies the Need to Limit Access in Verizon MA's COs.

In Exhibit AG-VZ 1, Verizon MA has provided evidence of security breaches *reported* to Verizon's Collocation Care Center ("CCC") and/or Verizon's Corporate Security Department[32] in Massachusetts and other jurisdictions from January 2000 to

---

[31] Although Verizon MA has always had security concerns with physical collocation, those concerns are exacerbated since September 11th. Exh. VZ MA 1, at 17. *See e.g.*, Michael K. Powell, Chairman, FCC, *Digital Broadband Migration Part II*, at 11, Remarks at FCC Press Conference (Oct. 23, 2001) ("Securing Our Nation's Communications Infrastructure" is a "Principal Objective" of "Homeland Security"), *at* www.fcc.gov/Speeches/ Powell/2001/spmkp109.pdf; *see also* Young & Berman, *Exposed Wires: Trade Center Attack Shows Vulnerability of Telecom Network*, Wall St. J., Oct. 19, 2001. Exh. VZ MA 1, Att. 2..

[32] Verizon and carrier personnel are advised to contact either the CCC or Corporate Security to report alleged security violations. Tr. 327-28, 328, 353, 365-66, 371; Exh. AL-VZ 2-10. Upon receiving a report of a "CO security breach," the CCC logs in the call, assigns a ticket number, prepares a description of the matter, and refers the information to Corporate Security for investigation. Exh. AG-VZ 1-1. The CCC also enters the information into a database for record-keeping purposes. Corporate Security would then gather additional facts by dispatching an investigator to the actual location to review the physical conditions and/or interviewing any available witnesses. Exh. XO-VZ 1-2. Corporate Security reports its findings to the CCC, which then notifies the carrier.

Depending on the nature of the incident, Corporate Security would also inform and/or assist the police, as needed. Tr. 307, 314. In cases of theft or vandalism to a carrier's collocation arrangement, the carrier is advised to file a police report. If Corporate Security is contacted during the commission of a crime (*e.g.*, assault and battery, breaking and entering, theft, etc.), Corporate

April 2002. That Exhibit documents the following types of security violations in Verizon's collocated COs across the country:

- ?? unauthorized entry into CO areas outside of the carrier's collocated equipment space;
- ?? theft and vandalism of carrier equipment resulting from unauthorized access to a carrier's cage;
- ?? theft and vandalism of Verizon equipment in secured and unsecured areas of the CO;
- ?? cables cut on frames;
- ?? carrier entry without an authorized ID badge or electronic access card;
- ?? carrier entry with unauthorized use of another's ID badge or electronic access card;
- ?? doors propped open or locks taped; elevators doors held open;
- ?? carrier tapping Verizon's phone lines;
- ?? broken locks on doors or collocation cages, card readers destroyed, or power systems disabled due to vandalism;
- ?? unauthorized carrier testing on Verizon's side of the equipment or plugging modem into Verizon's AC outlet;
- ?? carrier running extension cords across the CO floor and/or past Verizon's equipment;
- ?? carrier rummaging through Verizon's parts cart;
- ?? carrier removing Verizon property;
- ?? carrier using cell phones within the CO, which is prohibited because of technical interference with network operations;
- ?? carrier improperly or unsafely disposing of rubbish in the CO collocation area .

Security would immediately notify local police or other law enforcement official regarding this life-threatening situation. Tr. 305, 310. Finally, Corporate Security would monitor sites for repeat incidents and, if a pattern is identified, take additional steps, such as site surveillance, camera installation, site hardening, etc. Exh. XO-VZ 1-2; Tr. 688.

Exh. VZ MA 1, at 22; Exh. AG-VZ 1; Exh. DTE 1.

Although those *reported* security violations may not be all-inclusive,[33] they demonstrate the types of security breaches that occur with "greater" foot traffic within the CO and the harm or damage that can result to Verizon's and/or collocators' equipment or facilities. Tr. 63, 73, 375-76. This includes, in some cases, service outages affecting thousands of customers.[34] *Id*. Verizon's Security experts stated without contradiction that each of the listed security violations is a serious infraction that poses a direct threat to the safety and reliability of Verizon's network. Tr. 375-78.

Because these incidents occurred *within* Verizon's COs and could have affected *any* facilities that run through those offices, the potential for significant network damage and service interruptions for both Verizon MA and collocators is substantial. Tr. 349, 367, 379. For example, a carrier's removal of Verizon's test set needed to troubleshoot problems could prolong Verizon's restoration of a service interruption or disruption in the network. Tr. 379. As a result of unauthorized carrier testing on Verizon's side of the equipment, a carrier could also reverse or cross pairs, thereby disrupting service. Tr. 379. This could ultimately interfere with phones needed for Verizon to communicate with

---

33 It is a reasonable assumption that not all security violations are reported to the CCC or Corporate Security. Tr. 45. Moreover, in gathering the CCC data, Verizon used the category "CO security breach," which would include alleged vandalism, break-ins, theft, sabotage, etc. Tr. 72, 373; Exh. AG-VZ 1. Likewise, Corporate Security identified incidents relating to "CLEC" or "collocator." Tr. 669. Any reports that were classified differently would not be captured in this data search.

34 Verizon is aware of at least one instance in Washington state where a security violation – (*e.g*., the CLEC worked on Verizon's Battery Distribution Fuse Bay ("BDFB") in a secured area to turn up power in its collocated equipment) - caused a service outage in a remote switch, interrupting service to approximately 9,000 customers. Exh. AG-VZ 1, Att. 3; Exh. VZ MA 1, at 22 n.19. In addition, Verizon has experienced cases where the collocators' personnel have broken into locked power rooms in the Company's CO in an attempt to work on power distribution equipment (*e.g*., the power distribution panel), creating a serious safety risk as well as the potential for widespread service interruptions. *Id*. Fortunately, these failed attempts to work on Verizon's power equipment did not result in injury to the workers or cause damage to the network. *Id*.

other technicians and support centers to correct the problem. Tr. 379. Likewise, a carrier's improper – or unauthorized – procurement of Verizon's plug-in units or cards could interfere with Verizon MA's provision of service and damage its facilities. Therefore, the ramifications of the above security incidents are far-reaching, and warrant adoption of Verizon MA's collocation security proposal to limit access or foot traffic in the COs. Tr. 60, 63.

Contrary to some parties' claims, it would be imprudent for the Department to wait until major service-affecting outages occur – or a particular number of security violations in Massachusetts is reached - before approving Verizon MA's proposal to enhance security measures in collocated COs.[35] Tr. 45; Exh. Sprint-VZ 1-4; Exh. VZ MA 2, at 4-5. The very purpose of the Department's investigation is to consider *proactive* steps to prevent such incidents. Tr. 44, 63; Exh. AL-VZ 1-25. By approving Verizon MA's collocation security proposal, the Department would enable Verizon MA to prevent these crimes and protect against future network harm that would be detrimental to Verizon MA, other carriers and end-user customers. Tr. 42.

C. Verizon MA's Collocation Security Proposal Is A Reasonable, Proactive Means of Minimizing the Potential for Network Harm.

[35] Some parties suggest that Verizon MA should conduct risk assessments on a per office basis in establishing its security plan. Tr. 124. That argument is fallacious.

First, a per CO risk assessment is not required because Verizon MA's collocation security proposal outlines an appropriate *baseline* plan for enhancing security in *all* COs. Second, the typical risk assessment examines whether a building is located in a high crime area to determine relative risk. The basic premise of such risk assessments may no longer be sufficient given the events of September 11th. Tr. 28. Third, it would be premature to perform risk assessments on "critical" offices because the Department has not yet approved the concept – nor designated which offices would qualify based on specific criteria. Tr. 63. Finally, it is ironic that parties, such as AT&T, have not completed risk assessments for their Massachusetts locations, given their position on this matter. Tr. 439.

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. Exh. VZ MA 2, at 6. 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. Each component of Verizon MA's collocation security proposal is designed to achieve that objective - with minimal impact on existing collocation arrangements.

Verizon MA's proposal is also consistent with applicable federal and state law. Contrary to parties' unfounded claims, Verizon MA's recommendations are neither anti-competitive nor discriminatory. Accordingly, Verizon MA's collocation security proposal is reasonable, appropriate and should be approved by the Department as filed.

1. Requiring Separate and Secured Space For All Types of Physical Collocation.

Verizon MA's current practice is to locate all types of physical collocation arrangements in separate and secured space in its COs, wherever possible. Tr. 363. This includes caged, SCOPE and CCOE arrangements.

Generally, when assigning and designing collocation space in the CO for other carriers, Verizon MA's engineers try to create separate and secured areas where there is no access to the Company's own equipment or where the Company can create a secured partition between its own equipment space and the collocation space. Exh. VZ MA 2, at 8. For example, once carriers enter their collocation area, their access to Verizon MA's equipment would be constrained by a wall, or in some cases a wire mesh partition, separating Verizon MA's equipment area from the collocation space. *Id*. Entry to the

Verizon MA's equipment area is also possible only through locked doors that a collocated carrier's building key or CRAS access card will not open. *Id*.

In its *Collocation Remand Order*, the FCC expanded Verizon MA's rights to separate and segregate physically collocated equipment within the CO premises. Exh. VZ MA 1, at 34. Verizon MA's current practices meet the FCC's conditions, as set forth in 47 C.F.R. §51.323(i)(4), for restricting physical collocation to segregated CO areas. The separated space is comparable, from a technical and engineering standpoint,[36] to unsecured space; is available within the same time frame; is provided at no added cost beyond the applicable, flat-rated space conditioning charge; and would be imposed on physical collocation space provided to a Verizon affiliate. 47 C.F.R. §51.323(i)(4)(ii), (iii), (iv), (v); Tr. 36-37, 243-47, 265-66.

Requiring separate and secured space for all types of physical collocation is warranted under FCC rules because of the "legitimate security concerns" raised by providing carrier personnel 24 hour a day, seven days a week unescorted access to Verizon MA's facilities in addition to access to their own collocation arrangements. 47 C.F.R. §51.323(i)(4)(i). A higher, yet reasonable, degree of security is required to ensure full network reliability, and can only be attained if collocators are located in separate and segregated areas of the CO. Tr. 350. Accordingly, the Department should permit Verizon MA to apply a general policy of *secure* segregation and separation of its equipment areas and collocator equipment areas in COs for <u>all</u> forms of physical

[36] The separated space is equipped with the appropriate power (both AC and DC), heat, ventilation, air conditioning, and lighting to enable the carrier's technicians to work on collocated equipment in that space. Tr. 247-48.

collocation, and allowed to migrate physical collocation arrangements that do not comply with that standard. Exh. VZ MA 1, at 27.

Providing a physical and secure barrier that prevents carriers or others from gaining access to Verizon MA's CO equipment is necessary for several reasons. First, while Verizon MA is permitted to escort its own vendors and contractors, carriers are allowed round-the-clock, unfettered access to the CO premises. Exh. VZ MA 1, at 23. It is virtually impossible to provide adequate security for Verizon MA's facilities in an *unsecured* environment under these circumstances. Exh. VZ MA 1, at 33. This leads to increased opportunities for accidental or intentional dislodging of Verizon MA's connections or damage to other company equipment or network facilities that are exposed and physically unseparated from collocators' equipment, as described above. *See* discussion *supra* Section III.B. It also increases the likelihood of sabotage and/or potential terrorist threats. Exh. VZ MA 1, at 28.

Second, for network safety reasons, Verizon MA requires that its own vendors adhere to the company's "Safe Time" policy. Exh. VZ MA 1, at 28. This prohibits equipment installation or rearrangement activities within close proximity to working equipment except during late evening to early morning hours (*i.e.*, typically between 11:00 P.M. and 7:00 A.M.) when any accidental disruption to working equipment would have the least impact on consumers. *Id*. That safety policy would be undermined, and network security threatened, if separating or partitioning collocator equipment were not required, and collocator personnel could access unsecured Verizon MA equipment any time of the day. *Id*.

Third, the number of collocators in Massachusetts COs range from one to as many as 27 carriers per CO. Each collocator, in turn, has many employees, agents and contractors, thereby increasing exponentially the sheer number of unfamiliar personnel who would potentially have access to Verizon MA's COs. Exh. VZ MA 1, at 22. Even if Verizon employees are in the CO at the same time as the collocators' employees, they would not necessarily know which collocators' employees belonged in a particular CO (especially with the unauthorized sharing of ID badges and access cards), or on which piece of equipment a given technician was authorized to work. *Id*. at 28. Physical separation of carrier collocation equipment area and Verizon MA's equipment areas would provide Verizon MA with a greater ability to deter or prevent unauthorized individuals from venturing beyond their designated area into areas where they have no reason or authority to be.[37] This provides further assurances that the network will be safer and better protected. Exh. VZ MA 1, at 28-29.

Fourth, Verizon's actual experience with carrier personnel suggests that the intermingling of equipment raises considerable security risks because of fundamental differences between Verizon MA's employees or vendors and carriers' employees or vendors, who would be installing and repairing equipment that is not physically separate from Verizon MA's equipment. Exh. VZ MA 1, at 30-31. For example, carrier personnel may have less incentive to exercise care with Verizon's or other collocated carriers' equipment, or may be less trained or less familiar with the CO environment, and less aware of the potential incidental harm to the various types of CO equipment. Exh. VZ MA 1, at 22; Exh. Conversent-VZ 1-17; Exh. XO-VZ 1-3..

[37] In fact, there are existing equipment areas in the CO where Verizon MA employees are restricted from entering, except for those employees who are properly trained to work on the equipment.

Unlike Verizon's own employees, carriers' employees are not accountable to Verizon MA.[38] Exh. VZ MA 1, at 30. Nor does Verizon MA control the level of training that the carriers' employees receive.[39] Many carriers have also opted to use non-approved or non-certified vendors in their collocation facilities and collocation common areas, resulting in increased incidents of standards and work practice violations within Verizon's COs.[40] Exh. XO-VZ 1-3; Exh. Qwest-VZ 1-38. Accordingly, both because

---

38 Verizon MA may escort a carrier employee out of the CO if he/she is unauthorized or responsible for accidental or intentional damage in the CO. However, Verizon MA cannot terminate his/her employment, as it could its own employee or contractor, for not following proper CO procedures or exercising due care in proximity of Verizon MA's equipment. Exh. VZ MA 1, at 30; Exh. AL-VZ 1-16. That distinction creates an incentive for Verizon MA's workforce and contractors to follow proper procedures and exercise care and caution when working around Verizon MA's equipment, and conversely a disincentive for carrier employees or agents. Exh.VZ MA 1, at 30. In fact, the carrier employee or agent can re-enter Verizon MA's CO at another time using someone else's access card, or may accompany a co-worker with a valid access card. *Id*. at 31.

39 Verizon MA has no way of knowing whether the carrier employee has been adequately trained to work on equipment in a CO environment. *Id*. Untrained carrier employee/agent may accidentally damage Verizon MA's equipment while working on the carrier's equipment, or may inadvertently work on Verizon MA's equipment in a commingled environment. Because carrier personnel generally are less familiar with the CO equipment than Verizon's employees, they pose a greater security risk, and thus are more likely to commit some unintentional act causing damage or harm to the network. Tr. 112.

By contrast, Verizon MA's technicians are highly trained. Exh. Conversent-VZ 1-17. Verizon's own employees undergo significant training before they are permitted to work in the CO, and some are even specifically trained and authorized to work on particular CO equipment. Tr. 738. Such training includes a combination of courses, supervised "on-the-job" training, and exercises in sophisticated training lab environments where CO tasks are simulated and not customer-service affecting. Exh. Conversent-VZ 1-17. During 2001, Verizon CO employees completed an average of 49 hours of training. *Id*. In addition to an initial and progressive series of training courses, CO technicians become increasingly proficient in their job by gaining practical CO experience. They also receive upgrade training as new technologies and equipment are introduced in Verizon's COs. *Id*.

40 Because the non-approved contractors and vendors often do not know the CO requirements, they may hastily finish a job, causing problems with the office infrastructure. This can include careless or negligent acts, such as leaving installation debris after completing a job (an obvious safety and fire code violation and an expense to Verizon for removal), to life threatening safety violations (such as leaving fused and unterminated power cables) and network hazards (such as removal of fuses without proper authority or clearance). Exh. XO-VZ 1-3. Likewise, even when some carriers have their own technicians perform work in their collocation facilities, the same violations have occurred due to inexperience or lack of knowledge of applicable CO standards and requirements. *Id*.

Verizon MA can carefully screen and train its employees and because Verizon MA is better able to hold its own employees and vendors accountable, physical segregation of collocator equipment is necessary. This will minimize the likelihood that third parties with no legitimate business in Verizon's COs will gain access to them. Exh. VZ MA 1, at 31.

Finally, placing CLEC equipment in a separate and secured area of the CO away from Verizon MA's equipment may also have the added benefit of providing not only superior, but often less expensive, security arrangements for both Verizon MA and the collocator. This can allow easier access for the collocators' personnel and reduce the need for security cameras systems and other expensive security arrangements. Separate space that is dedicated to collocation can also be engineered with new collocation arrangements in mind, *e.g.*, to provide power and office connections likely to be requested by collocators. Exh. VZ MA 1, at 29.

Contrary to parties' claims, existing security measures, such as card readers, keys, and cameras, are simply not enough in a collocated environment where Verizon MA's and carriers' equipment are intermingled in the same unpartitioned, unsecured space. Exh. VZ MA 1, at 30. For example, video surveillance is often ineffective because when equipment is located in the same or adjacent bays, it is virtually impossible for an on-camera view to show on which piece of equipment a technician is working, let alone whether the technician has made inadvertent or intentional contact with equipment in an

---

For example, at a CO in Washington D.C., a vendor opted to drill holes into a concrete floor without first employing required dust abatement procedures. That negligent act resulted in the evacuation of the entire building, and the excessive dust jeopardized the operating equipment in the CO. Exh. AG-VZ 1, Attachment (summary document titled "Operational and Security Issues in Bell Atlantic Central Offices with Collocation," at 3).

adjacent bay. Exh. Conversent-VZ 1-12. Moreover, while video surveillance alone may provide some deterrent to interference with Verizon equipment, for the most part, it can only help determine accountability after the damage is done. Exh. VZ MA 1, at 30.

Even if such security devices *could* be reasonably placed in all necessary areas in the CO, any accidental or intentional damage to Verizon MA's equipment would be exceptionally difficult to detect, much less prevent, because of the close proximity of the carrier equipment and carrier personnel working on that equipment. Exh. VZ MA 1, at 30. In addition, much of the equipment deployed by the carriers looks the same as Verizon MA's equipment,[41] which increases the likelihood that carrier personnel may inadvertently work on the wrong shelf - and directly or indirectly cause a service outage. Accordingly, Verizon MA should be allowed to require that carrier equipment be separate and secure from the company's own equipment and not commingled, and to require virtual collocation where available floor space limits preclude establishing a separate, segregated area for physical collocation. Exh. VZ MA 1, at 31.

2. Requiring Relocation of Unsecured CCOE Arrangements or Conversion to Virtual Collocation

As stated above, although Verizon MA seeks to place all physical collocation arrangements (*i.e.*, traditional caged, SCOPE and CCOE) in separate and secured space, Verizon MA cannot require that CCOE or cageless arrangements be placed in a secured area of the CO. Tr. 144; *See* discussion *supra* Section III.A n.24. On a going-forward basis, Verizon MA recommends requiring that caged and cageless arrangments be located

[41] Verizon's actual experience nationwide in physically collocated COs suggests that when carrier and Verizon equipment are similar or the same, this increases the likelihood that spare parts on hand in Verizon's CO will be "poached" if needed by a collocated carrier for provisioning or maintenance. This too can result in service outages, as Verizon has experienced firsthand when carriers have taken in-use Verizon equipment parts for their own needs, without Verizon's permission or prior knowledge. Exh. VZ MA 1, at 30-31.

in separated space. Exh. VZ MA 1, at 33-34 This would enable Verizon MA to limit future cageless collocation arrangements to only those COs where Verizon MA has or can provide secured segregated space – and to close a CO entirely to all forms of physical collocation where separate space cannot technically be made available. Exh. VZ MA 2, at 10-11.

In addition, Verizon MA recommends that the Department permit the Company to require the relocation of *existing* unsecured CCOE arrangements to segregated space within a given CO – or, alternatively, the conversion to virtual collocation when separate and secured space is not available. Exh. VZ MA 1, at 29; Tr. 363. This is warranted under FCC rules (47 C.F.R.) because of the serious and "legitimate security concerns" raised by such configurations in a post-September 11th environment. Exh. VZ MA 1, at 32-33; Exh. VZ MA 2, at 11. As previously noted, there is only one cageless arrangement provided by Verizon MA – *i.e.*, the Hopkinton CO – currently located in unsecured space intermingled with Verizon MA's equipment in the CO. Exh. AL-VZ 1-1; Tr. 144-45; Exh. AL-VZ 1-9; Exh. AL-VZ 1-21; Exh. Conversent-VZ 1-20.

Verizon MA's proposal is also consistent with the Department's previous decision in D.T.E. 98-21 (*Covad Communications Company*), which rejected Covad's proposal for unsecured cageless collocation arrangements in Massachusetts. Exh. VZ MA 2, at 10-11. In its Order, the Department founf that physical collocation arrangements generally should be in separated, secured space. D.T.E. 98-21, *Order*, at 10-13 (June 5, 1998); Exh. Sprint-VZ 2-17. Likewise, in this proceeding, the Department should recognize that placing all physical collocation arrangements (including cageless) outside the "secure

envelope" is necessary to ensure the safety, security and reliability of the telecommunications network.

Contrary to some parties' claims, Verizon MA is not proposing to eliminate all cageless collocation, but only CCOE arrangements in areas that cannot be physically separated from Verizon MA's equipment areas.[42] Exh. AL 1, at 8; Exh. Sprint 1, at 9. Because unsecured CCOE arrangements pose unacceptable and unnecessary risks to the telecommunications network infrastructure, Verizon MA's proposal this is a reasonable approach and should be adopted by the Department.

3. Requiring Separate Entrances and/or Secured Pathways to Physical Collocation Areas

Even if a separate collocation room exists in a CO, Verizon MA's network facilities would not be adequately protected if a collocator has to walk *through* Verizon MA's equipment area to reach that separate and segregated collocation space. Tr. 146. In addition to the switching equipment, a Verizon CO contains critical pieces of equipment, such as power, fuse panels, and battery strings, that support the network.. Tr. 159-60. Therefore, unless Verizon MA can partition its facilities and equipment, the Department should permit Verizon MA to require a separate entrance and/or separate pathway for collocators to restrict their ability to traverse Verizon MA's equipment areas and gain access to Verizon MA's network facilities. Exh. VZ MA 1, at 17. Minimizing carrier access or "foot traffic" through Verizon MA's COs – and the number of people

[42] Currently, there are 37 Massachusetts COs where there is currently no separate, secure space available for physical collocation arrangements. Exh. Qwest-VZ 1-11; Tr. 727. This is a very dynamic process, and may change based on the following factors, *inter alia*: the inward and outward movement of each collocator in a CO; mergers resulting in return of existing collocation arrangements; future demand in a CO; building additions; equipment and/or infrastructure rearrangements; environmental conditions; etc. Tr. 344; Exh. AL-VZ 1-10. It would be virtually impossible to anticipate where or when another Hopinkton CO would arise. Tr. 344. This determination would be made at the time of the specific collocation request.

coming in contact with Verizon MA's network equipment, is warranted to reduce the potential risk of network harm. Exh. VZ MA 1, at 22-23. 27.

As described above, the FCC rules permit the establishment of separate entrances and pathways in the CO provided that certain conditions are met. 47 C.F.R. §51.323(i)(4). Verizon MA's proposal satisfies those requirements in that its recommendation is necessary to address "legitimate security concerns" or "operational constraints," is technically feasible, would not result in provisioning delays, and would have little or no additional cost impact on the collocators.[43] Therefore, the Department should permit Verizon MA to *require* separate entrances and/or separate pathways to provide physical collocation in a CO. Exh. Qwest-VZ 1-11.

Verizon MA's collocation security proposal reflects current practices in Massachusetts.[44] Tr. 36-37. Access to the separate collocation area in Massachusetts COs is generally by means of a secured corridor or pathway. That pathway would constrain access to Verizon MA's equipment area by separating the CO's ingress and egress route either by walls or, in some cases, a wire mesh partition with locked doors that other collocated carriers' building key or CRAS access card will not open. Exh. VZ MA 2, at 9.

---

[43] Under extraordinary circumstances, if Verizon MA incurred substantial costs to create a separate entrances or pathway in a CO, the Company may seek to apply a special construction charge to recover those costs from the cost-causer, *i.e.*, the collocated carriers. Tr. 266. Permitting Verizon MA to recover its additional security-related costs from the collocators is fully consistent with the longstanding economic cost recovery principle of cost causation. Exh. VZ MA 1, at 40. The special construction charge is a tariffed rate developed on a time and materials basis, pro-rated over the square footage, and applied proportionately to all carriers in a CO based on their collocated space. Tr. 267, 739. Verizon MA does not anticipate that this situation would arise, nor has Verizon MA ever applied or quoted such a charge in the past in Massachusetts. Tr. 740.

[44] Because the collocation process is dynamic, Verizon MA cannot predict what COs in the future – other than the Hopkinton CO - would be unable to meet the separate entrance and/or pathway requirement. Tr. 147; Exh. VZ MA 2, at 10.

If separate entrances and/or secured pathways do not exist in a CO, then Verizon MA currently seeks to construct alternate routes or separate entrances to meet the carrier's request for physical collocation. Exh. AL-VZ 2-8; Tr. 266-67. Should Verizon MA need to establish a separate entrance or pathway to secure its facilities, no charge would be imposed on the carriers because those costs are already captured in Verizon MA's non-recurring space conditioning or preparation charge that is applied upon request for physical collocation. Tr. 36-37; 265-66; *See e.g.*, D.T.E. Tariff No. 17, Parts E (§§ 2, 4, 6 and 9) and M (§ 5). Thus, there would be no cost impact on carriers.

Contrary to parties' claim, Verizon MA's proposal would not require collocators to use a different door (*i.e.*, separate entrance)[45] from Verizon personnel to enter the CO provided that a secured pathway exists. Tr. 148, 229. Indeed, in most Massachusetts COs, there is a common peripheral door into Verizon MA's COs that leads either directly to the separate collocation area or opens to a common vestibule area. Exh. VZ MA 2, at 9; Tr. 149, 230. Once inside the building, the collocators would then proceed through a different door, using either a key or an electronic access card, or down a separate passageway or secured corridor or pathway to access their separate physical collocation space. Tr. 148-49. Under those circumstances, Verizon and non-Verizon employees could use the *same* CO entrance because access to Verizon MA's network and equipment is segregated and secured. Tr. 230.

---

[45] WorldCom incorrectly claims that Verizon MA provided separate entrances for carrier personnel during work stoppages because of concern with potential Verizon MA employee misconduct. Exh. WCOM 1, 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. Exh. VZ MA 2, at 9. The Department has approved the practice of designating separate entrances for use during work stoppages. *Order*, at 5.

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. Exh. VZ MA 2, at 10. If the carrier inadvertently or intentionally takes the elevator to the wrong floor, the carrier's key or access card would not open locked doors leading to Verizon's equipment area. Once on the appropriate floor in Verizon MA's CO, the carrier's keys or access card will only open the door to the space where the collocation arrangement is located. *Id.*

Accordingly, Verizon MA's proposal is a reasonable collocation security measure, and should be adopted by the Department.

4. Providing Reasonable Access to Shared Facilities

The FCC's finding that collocated carriers are entitled to "reasonable access" to shared facilities in ILEC COs should not be construed as providing collocators with an absolute right to roam about the CO and traverse areas where Verizon MA's equipment is located to access those shared facilities. Exh. VZ MA 1, at 35; *Advanced Services Order*, ¶ 49.. Providing carriers with unfettered access to Verizon MA's facilities in the name of providing access to shared facilities would seriously undermine the FCC's rules allowing ILECs to restrict physical collocation to separate and secure space for security reasons. Thus, Verizon MA seeks Department approval to limit carrier access to shared facilities to where these facilities can only be accessed *without* entry to Verizon MA's equipment areas.[46] Exh. VZ MA 1, at 34; Tr. 226. Alternatively, Verizon MA may require escorts,

[46] For example, if carrier personnel come into a common vestibule in the CO and can access the restrooms at that point – or after passing through a security door or following a secured pathway en route to the segregated collocation space, then they will be given access to the restroom facilities. Tr. 224-25. However, if the carrier personnel must traverse Verizon MA's equipment

provided at the carriers' expense. Tr. 228. To do otherwise would compromise Verizon MA's ability to preserve and protect the telecommunications network by securing its equipment in a "secure envelope." Tr. 33, 225.

Verizon MA's proposal is consistent with its existing practices for carrier's use of shared CO facilities. Currently, authorized carrier employees, agents and contractors have – and would continue to have – reasonable access to CO common areas in accordance with FCC requirements and as described in Verizon MA's interconnection tariff (D.T.E. Tariff No.17, Part E, Section 2.2.5.A). That tariff provision states that "[t]he reasonable use of shared building facilities (*e.g.*, elevators, unrestricted corridors, designated restrooms, etc.) will be permitted." Exh. Sprint-VZ 1-20; *see also* Exh. Sprint-VZ 1-8. As a practical matter, no change would be required in Verizon MA's procedures, except for the Hopkinton CO, for the reasons stated above. Exh.AL-VZ 1-2; Exh. VZ MA 2, at 12.

Likewise, under its collocation security proposal, Verizon MA would maintain its current policy of coordinated, pre-arranged access at the carrier's expense for the use of temporary staging areas, loading docks, freight elevators or exterior building openings for vendor deliveries, unpacking, rigging and assemblage of carrier equipment in a given CO.[47] This would reasonably limit collocators' access to Verizon MA's equipment areas.Exh. VZ MA 2, at 11; Exh. Sprint-VZ 1-21. Verizon MA's procedures provide carriers with "reasonable access" to common areas during prearranged mutually

---

area to reach the restrooms, then Verizon MA must be permitted to restrict the use of those restrooms or require escorted access, if necessary, at the carrier's expense. Tr. 225.

[47] Exh. Sprint-VZ 1-8. *see also* Exh. Qwest-VZ 1-43, *citing* from Verizon's Wholesale Website - Method of Procedure (MOP) in Section 7 of the Network Equipment Installation Standards (IP-72201); *see also* Exh. Qwest-VZ 1-40; D.T.E. Tariff No. 17, Part E, Section 2.2.5.A.

agreeable time periods, and are comparable to Verizon MA's practices for coordinating access with its own for vendors for equipment deliveries and assemblage. Exh. AL-VZ 1-1; Tr. 226-27.

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. Exh. VZ MA 2, at 11.

5. Requiring Virtual Collocation at RT Locations

As explained above, unlike a CO, in most cases, it would be practically impossible to segregate Verizon MA's equipment into separate space in an RT. In fact, none of the approximately 2000 RT structures in Massachusetts are designed to enable Verizon MA to secure its equipment from access by other carriers. Exh. VZ MA 1, at 36, Att. 3. Moreover, the limited space in an RT exacerbates the potential risk of network damage because network facilities in an RT are more closely located with other facilities. *Id*. at 36.

In addition to the inherent structural difficulties with providing secure access to RT locations, there are considerable administrative and operational concerns to overcome. For example, access to the various types of RTs is controlled by various means, including padlocks, keys and special tools. Retrofitting RTs for other security mechanisms (*e.g.*, placing card readers or cameras) to give other carriers access would be a significant and costly undertaking. Exh. VZ MA 1, at 36-37. This also assumes that those methods alone would provide adequate network security – which they would not.

Indeed, the only way to ensure adequate security at an RT is to allow Verizon MA to limit collocation at RTs to virtual arrangements only. *Id*. at 37.

Virtual collocation will enable Verizon MA to reasonably protect its equipment because only Company technicians would be allowed to install and maintain equipment that the collocated carriers supply. This would make more efficient use of the limited available space because it eliminates the need to segregate equipment within the RT. Exh. VZ MA 1, at 37. It would also prevent one carrier's collocated equipment from being inadvertently affected by another carrier's technician working in the limited RT space. In addition, Verizon technicians are properly trained on taking necessary precautions in entering CEVs, which must be properly ventilated and checked for foreign substances (*e.g.*, gaseous odors) prior to entering the structure. *Id*. at 37-38.

Allowing only virtual collocation at RTs will not affect any existing collocated carriers because Verizon MA currently provides no collocation at RTs in Massachusetts. . Exh. VZ MA 2, at 12. Nevertheless, the Department should address the unique security problems raised by RT collocation - and the impracticability of other security measures (*e.g.*, separate space, partitioning, etc.) – and require virtual collocation in the event that RT collocation is requested in the future.[48] Exh. VZ MA 1, at 35-36; Exh. VZ MA 2, at 12.

Alternatively, if the Department does require physical collocation at RTs, which it should not, then the only practical means of protecting Verizon MA's network facilities is

[48] This would not conflict with existing FCC rules. The issue of RT collocation is currently under review at the FCC, and it is not known when the FCC will decide the issue. *See e.g., Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Order on Reconsideration and Second Further Notice of Proposed Rulemaking in CC Docket No. 98-147 and Fifth Further Notice of Proposed Rulemaking in CC Docket No, 96-98, FCC 00-297, at ¶ 104 (rel. Aug. 10, 2000) ("*FCC Reconsideration Order*").

to require escorts to accompany collocators that maintain their own equipment. Because of the greater possibility of accidental or intentional damage, collocators should not, however, be permitted to install their own equipment in RTs, even under a physical collocation arrangement. Exh. VZ MA 1, at 38.

Contrary to AT&T's claims, the use of escorts is necessary for RTs from the standpoint of security, and is permissible under current FCC rules. Exh. ATT 1, at 29; Exh. VZ MA 2, at 13. First, if the Department does not accept virtual only arrangements as a reasonable security measure, then escorts should be required because 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. *Id*.

Second, no current FCC rule prohibits an escort requirement at RTs. Exh. VZ MA 2, at 13-14; *FCC Reconsideration Order*, ¶ 104. Accordingly, the Department is not precluded from requiring escorts for collocation at RTs. Exh. VZ MA 1, at 37-38.

6. Requiring Virtual Collocation at Critical Offices

The final element of Verizon MA's collocation security proposal is the recommendation that it be allowed to offer only virtual collocation in those critical offices designated by the Department.[49] That restriction would also apply to existing physical collocation arrangements in those so-called "critical" offices, which would be converted to virtual arrangements in-place, if feasible. Exh. VZ MA 1, at 40.

---

[49] The other parties uniformly misunderstand Verizon MA's proposal. Verizon MA has proposed a process for determining which COs of its approximately 260 Massachusetts are critical - *not* the final result. Tr. 84-85, 341-42. Contrary to some parties' claims, Verizon MA's proposal would not "eliminat[e] physical collocation entirely." Exh. AL 1, at 8; Tr. 152. In fact, Verizon MA expects that a very limited number of COs would qualify as "critical." Exh. XO-VZ 1-4; Tr. 85, 232.

Although Verizon MA does not recommend specific criteria, the Department should consider various factors in determining whether a CO should be deemed "critical." Exh. VZ MA 1, at 14-17; Exh. VZ MA 2, at 14-16. They include the following:

- whether accidental or intentional damage to the network resulting in disruption of existing service in the CO 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[50] and other institutions that are involved in national security matters;

- whether failure of facilities housed in the CO has the potential to significantly disrupt communications involving critical entities (*e.g.*, nuclear power plant, a major airport facility, military installations, financial institutions, or emergency service providers, such as police, fire, or hospitals);

- whether the presence of an access tandem, E911 control tandem, or a Signaling Transfer Point ("STP") in a CO would significantly impact Massachusetts citizens either in a specific geographic area or statewide if telecommunications capability in that CO was lost.

Exh. VZ MA 2, at 15. Based on the type of customers and the nature of their business, the security and network reliability of Verizon MA's infrastructure in serving those select COs could be of national importance. Exh. VZ MA 1, at 39-40; Exh. AL-VZ 2-3. Likewise, the network equipment housed in Verizon MA's serving CO - and the critical nature of the traffic that equipment carries - may influence whether the Department designates a CO as a critical office. Exh. AL-VZ 3-4; Tr. 231, 260-61.

For instance, an access tandem is or can become a single critical point of failure in Verizon MA's network. In Massachusetts, an access tandem functions as the hub for

[50] Advanced technology companies (*e.g.*, data or data hotels) may be considered essential because of the nature of their operations to supply advanced communications and data processing capabilities to other entities in support of national security interests. Tr. 232.

many inter-office toll routes and as the final route for all other local and toll interoffice traffic when other routes are unavailable. Exh. VZ MA 2, at 15. In addition, many interconnectors, including CLECs and IXCs, rely on an access tandem to access Verizon's network. *Id*. 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. *Id*. at 16.

Unlike access tandems, neither an E911 control tandem nor an STP is a single point of failure in Verizon's network. In fact, both networks were designed in a redundant fashion so that there is no significant single point of failure. This is because both networks are extremely critical to the network and public safety. Exh. VZ MA 2, at 16.

There are four E911 control tandems in Massachusetts, [51] and each CO is connected to two of these tandems. Exh. VZ MA 2, at 16. However, even with this level of redundancy, accidental damage or a coordinated attack to one or more of these mated facilities has the potential to seriously disrupt emergency communications. *Id*. Likewise, a coordinated attack on the mated STPs that serve a LATA has the capacity to disrupt all interoffice traffic in a LATA. Accordingly, the security of E911 control tandems and STPs would be a high priority. [52] Exh. VZ MA 2, at 16.

---

[51] E-911 control tandems are located at the Medfield, Northampton, Wakefield, and Westborough central offices. Exh. AL-VZ 3-5. They are located in secure space separate from carriers' collocation areas. Carrier personnel would need key or card access to come in contact with these tandems. Exh. AL-VZ 3-5.

[52] Even if the access tandem, E911 tandem or STP is located in a separate room from collocation space, having carriers in close proximity to other network equipment in the CO can have a direct effect on the reliability of the network. Tr. 159-60; 164-65. This can have serious consequences – and, in some cases, life-threatening implications – for customers served by those COs. As an example, the battery distribution fuse bay ("BDFB") is located in common areas in the CO accessible by collocators. Tr. 400. Damage to the battery strings in the CO would cause a power

Moreover, by converting in-place existing physical collocation arrangements to virtual arrangements, Verizon MA would continue to provide a viable means for other carriers to interconnect for the exchange of traffic and access to Verizon MA's unbundled network elements in those critical COs - while minimizing the foot traffic and associated network risks. Exh. VZ MA 2, at 17; Tr. 116-17.

Finally, as discussed above, nowaiver or modification of FCC rules (47 C.F.R. § 51.323) would be required for the Department to establish virtual-only critical offices. *See* discussion *supra* Section II.A. Accordingly, Verizon MA urges the Department to support the concept of identifying critical COs for security reasons, and approve its collocation security proposal, as filed. Verizon MA would then work with the Department to establish the appropriate criteria for determining which specific COs are critical. Tr. 155, 261-62; Exh. VZ MA 2, at 16, 27.

D. Verizon MA's Enhancement of Its Existing Security Methods Alone Is Inadequate As a Preventive Measure.

Verizon MA uses a combination of various security methods in providing carriers with access to their collocated space and shared facilities within Verizon's COs.[53] Those security measures include the following: (1) non-Verizon employee collocation ID

---

outage and cause the tandem (access, E911, etc) to go down. Tr. 164-65.

Likewise, fire, water or other environmental damage – whether accidentally or intentionally caused by collocated carriers - would affect - and potentially interrupt – telecommunications services (including E911 services) in the CO. Tr. 159-60, 164. Damage to toll transmission equipment in common areas accessible to the colllocators could also affect service since that equipment supports trunks going to and from the E911 tandem. Tr. 165. Accordingly, these factors must be considered in determining whether to classify a CO as "critical" – even if the carriers have no direct access to the tandem or switch in a CO.

[53] While on Verizon MA's premises, collocators and their authorized employees, agents and contractors who have a legitimate need to access the carrier's physical collocation arrangement must abide by all Verizon security and safety practices. Violators of Verizon's current practices, which are posted on the Company's website, are subject to removal and termination of all access privileges. Record Request ATT-VZ 2.

badges; (2) electronic CRAS; (3) key-controlled access systems; (4) directional signage and floor markings (*e.g.*, floor tape); and/or (5) access through guarded entries. Exh. AL-VZ 1-4. In addition, Verizon MA may deploy security cameras, *i.e.*, Closed Circuit Television ("CCTV"), in COs with unsecured CCOE arrangements or where access to shared facilities is only available by means of unsecured open passage through Verizon MA's equipment areas. Exh. VZ MA 1, at 16-17, Att. 1.

Nevertheless, while Verizon MA's current security methods afford some protection and may even deter some security violations, they primarily enable Verizon MA to detect and respond "after-the-fact." Exh. VZ MA 1, at 18. Therefore, Verizon MA's planned enhancements to those current security measures, as described below, or other potential enhancements will not alone prevent some individuals from causing either intentional or unintentional damage to Verizon MA's network. Exh. VZ MA 1, at 26; Tr. 114. Verizon MA must also be allowed to take more *pro-active* steps to protect its infrastructure — the integrity of which is critical for the reliable, uninterrupted provision of voice, data, and emergency telecommunications services to the public, as outlined in Verizon MA's collocation security proposal. Without taking such *preventive* action, the potential personal and financial loss to consumers and businesses, including other carriers and governmental entities, could be substantial and far-reaching. Exh. VZ MA 1, at 18.

1. Requiring Background Checks Prior to Issuing Non-Verizon Employee Identification Cards

Verizon MA has taken steps to reduce "foot traffic" by restricting who is allowed to access COs and other company facilities. Only those individuals with a legitimate business need are permitted access to COs, and only with proper ID badges, access cards, and/or escorts, where applicable. Exh. AL-VZ 3-1. In an effort to better protect the

network since September 11th, Verizon MA has strengthened its CO security procedures by requiring that carriers conduct more extensive criminal background checks and drug screening of their employees and provide certification to Verizon before authorized ID badges or access cards can be issued. Exh. VZ MA 1, at 5. This is comparable to Verizon MA's pre-screening process for its own employees. Tr. 96, 101.

As part of its enhancement of security methods, Verizon MA adopted, effective in August 2002, the following pre-screening process for collocator personnel and their agents: (1) collocator certification that it has conducted a criminal background check of its employee and/or contractor dating back not less than 7 years in the county of residence, or previous county of residence; and (2) collocator certification that it has conducted employee drug screening to scan for the presence of controlled substances, as listed on the current Verizon non-employee access credential application.[54] Exh. AL-VZ 1-2. This reflects Verizon's policy to increase its criminal and drug screening requirement from five to seven years.[55] Tr. 127. It also places the responsibility on the collocators for certifying compliance with those requirements for its employees and agents applying to Verizon MA for access credentials. Tr. 103, 128-29.

Verizon MA reasonably assumes that collocators already have procedures in place to screen their employees for criminal backgrounds and drug use at the time of hire. Tr.

---

54 In addition, Verizon is currently in the process of working with its contractors to adopt a pre-screening process on a going-forward basis. Exh. AL-VZ 1-2; Exh. AL-VZ 1-17 (supplemental). Tr. 95, 97. Verizon's vendors are also responsible contractually for any harm resulting from their actions. Exh. AL-VZ 1-2.

55 Verizon MA does not believe that these background checks provide insight into whether an individual will engage in network-affecting conduct. Tr. 115. In addition, past criminal convictions would not necessarily disqualify an individual. Tr. 203. This would depend on several factors, such as the nature and date of the offense, and whether there were any mitigating circumstances (*e.g.*, self-defense). Tr. 204-205.

104, 264-65. Therefore, it is unlikely that this certification requirement would result in additional costs for any collocators in Massachusetts.

Contrary to some parties' claims, Verizon MA has established reasonable and effective procedures regarding the use of ID badges and access cards. Exh. Qwest 1, at 19, 22, 23; Exh. VZ MA 2, at 23. Those procedures apply to both collocators' and Verizon's employees and contractors. Exh. VZ MA 2, at 23. When in Verizon COs, all collocators and their representatives must use authorized access credentials or visibly wear ID cards or badges when in Verizon MA's COs. The collocator is also required to return the ID badge and access card of former employees or contractors upon termination of their employment. Exh. AL-VZ 1-1, Att. 2 at; 7-9; Tr. 716.

However, notwithstanding Verizon MA's long-standing policy of requiring collocators to return access credentials that are no longer required, that procedure is seldom followed, as the parties themselves admit. Tr. 411 (Allegiance); 508-09, 551-52, 596 (WorldCom); *see* Exh. VZ MA 2, at 23.[56] Verizon policies are publicly available on Verizon's web site, and are updated in industry letters sent to carriers via electronic mail. Tr. 573 (Covad), 612 (Qwest). Yet, carriers routinely ignore those existing policies, with few exceptions.[57]

Since carriers typically do not inform Verizon that that an ID is no longer required – but "not returned," Verizon MA may not know - until the card is not renewed and thus

---

[56] By contrast, Verizon MA confiscates ID badges and access cards of its former employees and contractors upon termination of their employment. Tr. 730. This prevents them from gaining unauthorized access after their employment has ended.

[57] To its credit, Qwest affirmatively keeps itself informed concerning Verizon's collocation policies and communicates those policies to its field personnel. Tr. 600-02.

automatically expires one-year from the date of issuance.[58] Tr. 411, 716. Although the carriers have the ultimate responsibility to control and properly enforce security procedures among their own employees and contractors, their failure to comply with Verizon MA's policies substantially diminishes the effectiveness of Verizon's security measures.[59] Exh. VZ MA 2, at 23.

2. Expanding Deployment of CRAS to Provide Access to Verizon MA's COs

Currently, all Verizon MA COs are secured either by a key lock or electronic CRAS.[60] Exh. VZ MA 2, at 22. Within the CO, access to Verizon MA's equipment areas and almost all separate collocation areas is also through locked entries – opened either by a key or access card. *Id*. The only exception, as noted above, is the Hopkinton CO.

As part of an overall plan to expand the number of COs where CRAS is used, Verizon expects to complete its deployment of CRAS throughout Massachusetts during

---

58 Once a card has expired, the user is no longer able to access the CO utilizing that card. To reinstate the expired access card, the CLEC must submit a renewal application to Verizon MA. When cards are reported as "lost," the CLEC is required to submit a replacement application. Exh. AL-VZ 1-6.

59 Since 1999, Verizon has issued more than 15, 000 ID badges and access cards of the type used in Massachusetts to carrier employees and contractors. Tr. 733.

60 As set forth in Section 2.6 of Verizon's Collocation Guidelines, Verizon provides a total of five keys per each facility entrance and/or common area to specific collocator management personnel for dispensing on an as-needed basis to individual employees. Exh. AL-VZ 1, Att. 2, at 8-9. The collection and assignment of keys are the responsibility of the collocator management personnel. Duplication of keys is prohibited. *Id*. at 8. All keys remain the property of Verizon, and must be returned when a collocator vacates its collocation arrangement. *Id*. at 9.

By contrast, Section 2.5 of the Collocation Guidelines states that Verizon issues a CRAS card to the individual collocator employee once a valid Verizon non-employee collocator identification card is issued and upon completion of a CRAS application form with collocator supervisory approval. Exh. AL-VZ 1, Att. 2, p. 8. CRAS cards remain the property of Verizon and cannot be "borrowed, transferred or otherwise used by anyone other thant the CLEC employee to whom it was issued." *Id*. Because a CRAS card is assigned on an individual employee basis, it must be returned by the collocator to Verizon upon the termination of the individual's employment. *Id*.; Tr. 715.

the next 18 months.[61]. Exh. Qwest-VZ 1-20 and 1-21. Tr. 110. CRAS is preferable to key locks because it provides Verizon MA with a record of who enters the CO. Tr. 110, 283; Exh. VZ MA 1, at 20. However, this security method is not foolproof.

First, Verizon MA is aware of carrier personnel or agents using cards belonging to others.[62] Exh. VZ MA 1, at 20. The ability to "share" access cards renders them useless at identifying who is in the CO and determining responsibility for damage to the network. Moreover, even if access cards are used properly, they may only provide Verizon with a witness or suspect for accidents or intentional bad acts. Tr. 283. Because the negligent use or misappropriation of access cards is undetected until "after-the-fact," access cards may have limited use as either a practical or effective pro-active security measure. Moreover, in the future, carrier personnel could also be compromised by giving CO access to an outside entity that is not authorized to enter Verizon's CO and does not understand the disruption or damage that could be done to critical facilities by certain activities. Exh. VZ MA 1, at 20.

Second, as noted above, Verizon MA is aware of instances in which CLECs have not reported lost access cards or returned cards given to former employees and

---

61 Approximately 34 Massachusetts CO are already equipped with CRAS, and Verizon MA plans to deploy this in an additional 27COs in 2002. Exh. Qwest-VZ 1-21; Exh. Qwest-VZ 1-20; Exh. VZ MA 2, at 24-25. The average historical, estimated cost for deploying CRAS in a CO is approximately $30,000 per CO. However, CRAS costs may differ based on individual characteristics of the CO, *e.g.*, size of CO, number of collocators, location of collocation arrangements, etc. Exh. Qwest-VZ 1-22. In addition, every door (peripheral, internal, etc.) equipped with CRAS would require a separate card reader at an additional cost. Tr. 278, 280-81. Carrier personnel would only be assigned access cards to the peripheral door to the CO, and any doors required to enter the separate collocation space. Tr. 712.

62 For example, there have been incidents where CLEC employees have entered the CO without an authorized identification badge, but with another CLEC employee's electronic access card. Moreover, at many Verizon MA COs, secondary exits are not monitored since they serve solely as exits. Such breaches, however, often go undetected and unpunished because Verizon does not have the same recourse against CLEC violators as it does with its own employees or vendors (*i.e.*, Verizon cannot discipline a CLEC violator or terminate his/her employment).

representatives. Exh. VZ MA 1, at 20; Tr. 356-57. Third, using CRAS will not prevent "tailgating," where someone with proper authorization opens a door for another entrant, thereby bypassing any security control point, sign-in log or CRAS that would restrict access to Verizon MA's space in the CO.[63] Exh. AL-VZ 1-7. Because the tailgater walks in behind another individual without swiping an access card across the card reader, the CRAS would not acknowledge that the tailgater is even in the building. Tr. 259-60. Verizon's Collocation Guidelines instruct collocator personnel and contractors to deny access to any individual or tailgater who attempts to enter the CO through a secured door and who does not display the proper and currently valid Verizon-issued access ID card. Every individual authorized to access the CO is responsible for following those guidelines to ensure the security and safety of the facility. Exh. AL-VZ 1-8.

Finally, CRAS does not show when an individual leaves a CO, thus making it impossible to determine the duration of an individual's stay or if he/she was in the CO when a security breach occurred. Exh. VZ MA 1, at 20-21; Tr. 359-60. Although an "anti-passback" – or "swiping out" – feature could be provided for access cards, this is not advisable.[64] Tr. 284-86.

---

63 Verizon MA is aware of two devices - turnstiles and mantraps – that may be utilized to deter tailgating. Tr. 291. Turnstiles are a barrier type of device that only permit one person at a time to pass through an opening upon that person activating the device with an authorized electronic access card. Mantraps provide a similar function by providing a full barrier in front of and behind the person with only enough space for one person in between the barriers. Both barriers must be activated independently, or in sequence by an authorized electronic access card. Exh. AL-VZ- 2-7.

Verizon MA does not believe that either of these methods are feasible or practical in Massachusetts. Sufficient additional space is required to install turnstiles and mantraps in a location. In addition, unless guarded, single-arm turnstiles can be bypassed by simply climbing over them. Multi-bar or gated turnstiles and mantraps would also impede technicians attempting to pass through with bulky supplies, test set gear or tools. For these reasons, Verizon MA has not implemented either of these measures in its Massachusetts central offices. Exh. AL-VZ- 2-7.

64 It should be noted that AT&T admitted that it does not utilize use a "swipe-out" feature on its

For example, if a collocator employee does not properly "swipe out" upon leaving the CO, then that employee's access card would be automatically invalidated and not provide access to re-enter the building[65] or to enter another Verizon MA building. Tr. 287; Exh. VZ MA 2, at 24. The access card would need to be reported as non-working, and reset by Verizon MA to permit any future use. Exh. XO-VZ 1-1; Exh. VZ MA 2, at 24. This is a time-consuming process, and would be an administrative and operational inconvenience for the collocator, by interfering with the collocator employee's ability to obtain 24 hour access, seven days a week to the CO. Moreover, even a "swiping out" requirement would not provide an accurate record of individuals leaving the CO if tailgating continues to occur when exiting the CO. Tr. 286.

In short, although security access cards are intended to prevent unauthorized personnel from accessing certain sections of the CO and to provide Verizon MA with a record of who enters its offices, they do not necessarily and conclusively identify the "user," And cannot prevent unauthorized access in all areas. Exh. VZ MA 1, at 20. Collocated carriers have not consistently and diligently followed Verizon MA's policy of returning authorized ID badges or access cards when an employee has terminated employment with the collocated carrier, nor have collocators been consistent in reporting stolen or lost cards on a timely basis (if at all). Exh. VZ MA 2, at 22. Accordingly, CRAS is simply not a sufficient mechanism to protect the CO from unauthorized entry and accidents or damage to the network infrastructure. In fact, CRAS can only be used

---

access cards in Massachusetts - although AT&T recommended that Verizon use that feature. Tr. 436-37; Exh. AT&T 1, at 14; Exh. VZ MA 2, at 24.

[65] Even the inadvertent failure of a collocator's technician to swipe his access card upon exiting the CO (*e.g.*, for lunch or to obtain a part from the truck to complete work repairing a customer trouble) would temporarily prevent that technician's return to perform further service activities in the building. Exh. VZ MA 2, at 24.

effectively in conjunction with physical barriers or partitions that separate carriers' and Verizon MA's equipment space and prevent unauthorized access to or through Verizon MA's equipment areas in the CO.

3. Other Security Measures

Some parties contend that rather than adopting Verizon MA's proposal, the Department should require Verizon to more effectively use cameras or CCTV to monitor and prevent undesirable conduct, making Verizon's proposals in this case unnecessary. Exh. ATT 1, at 14; Exh. Sprint 1, at 13; Exh. VZ MA 2, at 21. Their position is without merit.

The use of cameras *alone* is neither an effective nor efficient pro-active security method. Exh. VZ MA 1, at 18-19. Multiple cameras positioned in many locations throughout a CO would be required to capture all potential activity – and even then it would be virtually impossible to capture *every* angle in a CO to prevent or even sufficiently deter potentially harmful activity.[66] Also, the number of individuals required per CO to observe the video screens with real-time monitoring would be substantial and extremely costly both to Verizon MA and the collocators. These problems are compounded by the need to monitor many COs.[67]

---

66 It is particularly difficult for cameras to cover reasonably all portions of a physical facility in a CO environment, where many obstructions (*e.g.*, tall equipment bays and line-ups, ladders, and bulky equipment) may block the camera's view and make it impossible to determine precisely what an individual is doing. Indeed, even if enough cameras were installed to capture *every* angle in a CO, the quality and/or distance of the picture would simply not be sufficient to capture an individual's precise movements, and may not even be sufficient to determine the exact piece of equipment being worked on or tampered with. Exh. VZ MA 1, at 19-20.

67 For example, since carriers can access COs 24 hours a day, seven days a week, a minimum of four guards per collocated CO (or one per shift) would be required to provide real-time monitoring. Moreover, to prevent incidents from occurring, the posted guard must be sufficiently knowledgeable to identify suspicious activities, and adequately trained to intervene if an illegal or disruptive action is observed. Exh. VZ MA 1, at 19-20.

More important, although cameras may be useful to record events – and even deter criminal activity in certain cases, cameras *alone* are not enough as a pro-active security measure to prevent unauthorized access to a physically collocated CO environment. Exh. VZ MA 1, at 19, 21-22. Even real-time monitoring through the use of camera surveillance will not necessarily improve security in the central offices because not all activity can be captured due to the physical configuration of equipment and space in those locations, and sometimes obstructed views. Exh. Conversent-VZ 12. Therefore, while real-time monitoring may act as a deterrent for some individuals, the drawback is that it will not necessarily prevent actual security violations once the perpetrator is in the CO.

Contrary to the parties' claims, surveillance cameras do not address the underlying problem, *i.e.*, the real security concerns raised by affording collocators round-the-clock, unlimited access. The most effective security measure is to restrict access by non-Verizon personnel to certain parts of the CO (*e.g.*, outside the designated collocation areas) or, in the case of critical COs, allow no physical access at all.[68] Exh. Conversent-VZ 1-12.

---

[68] Even if security guards were posted in each CO (a very costly undertaking), this would not reduce the foot traffic through the COs, which is the primary culprit in causing inadvertent and intentional network damage. Tr. 157. Further, although most COs do not have assigned security guards, Verizon technicians are present in the collocated COs. Exh. AL-VZ 1-4; Tr. 134-37.

Moreover, contrary to some parties' suggestion, biometric devices (*e.g.*, fingerprint detector, signature analyzer, retinal scanner, or voice recognition equipment) are neither practical nor reliable security measures at this time. Exh. AL-VZ 2-4.

First, they can only compare the features of individuals scanned with profiles stored in a specific database. Second, they can produce inaccurate scanning results (*e.g.*, false positives), or the system can be fooled by latent prints (*i.e.*, when someone lifts a fingerprint image from a surface and then uses it) or physical disguises. Third, biometric devices can be slower than standard access system methods, such as electronic card readers, and, in some cases, are prone to malfunction. For instance, thumbprint or hand scanner surfaces must be kept clean and free of body oils and other debris build-up to function properly. Exh. AL-VZ 2-4. Finally, it is Verizon's

Verizon MA believes that combining the above expansion and enhancement of Verizon's existing security methods in Massachusetts with the establishment of Verizon MA's proposed collocation security plan will best meet the needs of protecting and preserving the telecommunications network infrastructure against deliberate and/or unintentional harm. No party has demonstrated any tangible detriment to competition if Verizon MA's collocation security proposal were adopted. Exh. VZ MA 2, at 25-26. Nor have they provided any evidence that Verizon MA's proposal is unlawful or discriminatory, or that it would increase service disruption or impose substantial additional costs, if adopted. *See e.g.*, Exh. Sprint-VZ 2-20; Tr. 222-23.

E. The Other Parties Present No Viable Alternatives that Would Enhance Security of the Network Infrastructure.

While the other parties devote great effort in criticizing Verizon MA's proposal to enhance security in Verizon's COs, they have offered few, if any, helpful suggestions of their own. Some advocate merely maintaining the status quo. Exh. AL 1, at 3; Exh. AT&T 1, at 6; Exh. Covad 1, at 21; Exh. WCOM 1, at 29. That is unacceptable in today's world, and fails to address properly the intent of the Department's investigation.

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 consider steps that could be taken to prevent harm before it occurs; it is

---

understanding that pilot programs and trials are underway to improve the accuracy and reliability of biometric devices. Until further testing is conducted and the value and effectiveness of these devices are proven, it would not be prudent to invest in biometric technology. In addition, biometric devices may be considered invasive, thereby raising serious privacy concerns. Exh. AL-VZ 2-4.

completely inappropriate and irresponsible to wait until a serious event occurs before taking action.

Several parties unremarkably recommend that the Department adopt whatever measures are developed by national task forces, such as the Network Reliability and Interoperability Council ("NPIC") and the National Security Telecommunications Advisory Committee ("NSTAC"). *See e.g.*, Exh. Qwest 1, at 7; Exh. Sprint 1, at 5. While those task forces are performing an important national function, the Department can and should evaluate measures that can be implemented in Massachusetts now to enhance network security. [cite HO's order denying motion to defer]

Some parties suggest that the only action that is necessary is for Verizon MA to more effectively implement existing security procedures. Exh. Qwest 1, at 19; Exh. ATT 1, at 6. They are incorrect.

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. Also, as explained above, while other security measures, such as additional cameras and similar surveillance equipment, can provide a degree of enhanced security, they will not deter all individuals from committing criminal acts.

Moreover, security devices must be properly used to be effective. Tr. 507. Collocators frequently do not use these devices properly, thereby substantially diminishing their effectiveness, for example, by misuse and misappropriation of access cards and failure to comply with Verizon MA's policy regarding return of unneeded cards. Exh. VZ MA 2, at 23; *see* discussion *supra* Section III.D.1.

AT&T claims that 90 percent of security breaches are attributable to "people" or "policy" failures. Tr. 462-63. If that is true, then it is clear that the carriers' repeated disregard of Verizon's policies calls for stricter security measures than mere enhancement of existing equipment and procedures — such as the mandatory separation of all carrier equipment from Verizon MA's equipment in all cases.

F. Virtual Collocation Is Recognized As A Viable Arrangement.

As stated above, under Verizon MA's collocation security proposal, virtual collocation would be required in certain critical offices, in RT locations, and in COs where no separate and secured physical collocation space is available. The parties object to that requirement because they contend that virtual collocation is not a viable arrangement. That argument is a red herring.

Virtual collocation is recognized as a viable option by the FCC and under the Act. 47 U.S.C. § 251(c)(6). It is technically feasible, and is is used by a number of collocators in Massachusetts. Indeed, in some cases, is the preferred method even when physical collocation is available. Tr. 739. This belies the parties' unsubstantiated claims that virtual collocation is not a viable arrangement.

The parties that oppose Verizon MA's proposal have presented scant and outdated anecdotal testimony regarding their allegedly negative experiences with virtual collocation in jurisdictions other than Massachusetts. They have provided no evidence regarding Verizon MA's provision of virtual collocation.As the Department is aware, there have also been few complaints regarding Verizon MA's performance related to virtual collocation. Exh. VZ MA 2, at 17. In fact, when Rhythms Links raised performance issues in connection with Verizon MA's virtual collocation performance during Verizon MA's Section 271 inquiry, the parties, at the direction of the Department,

successfully investigated and resolved the problem, as indicated in a joint letter filed in that matter. *Id.*, Att. 1. Moreover, Verizon MA has gained considerably from its experience with its former structurally separated data affiliate, Verizon Advanced Data Inc. ("VADI"), in provisioning virtual arrangements for Digital Subscriber Line ("DSL") and other advanced services from late 2000 to April 2002. Tr. 51, 93, 737. Verizon MA provisioned and maintained over one hundred virtual collocation arrangements for VADI in Massachusetts during that period. All of the other parties' experience with the provisioning of virtual collocation predates VADI and the knowledge, experience, and skill gained there. Tr. 409-10.

Unlike physical collocation, a virtual collocation arrangement does not require Verizon MA to assign a portion of the floor space in the CO to the collocated carrier for its exclusive use to install, operate and maintain its own equipment. Rather, the carrier leases its equipment to Verizon MA to install, maintain, upgrade and repair on Verizon's premises under the direction - and for the benefit – of the carrier. Exh. VZ MA 1, at 10-11. Despite these apparent differences, virtual collocation is similar to physical collocation in several ways.

First, contrary to Covad's claim, new installations for both physical and virtual collocation are provided based on a 76 business day interval in Massachusetts. Exh. VZ MA 2, at 18; Tr. 548 (Covad).[69] In fact, at the end of that period, the carrier must then install its equipment in a physical arrangement, while in a virtual arrangement the carrier's equipment would be in place. Tr. 548-49.

[69] In both cases, the collocator would have to order transport; but transport is ordered in the same way and at the same time intervals for physical and virtual arrangements in Massachusetts. Tr. 549-551.

Second, although a carrier cannot directly access the virtually collocated equipment, it can establish systems comparable to those used in a physical collocation environment to access remotely its virtually collocated equipment to perform various functions. Exh. VZ MA 1, at 11. This enables the carrier remotely to monitor and test its equipment, conduct diagnostics, and perform some maintenance activities – just as the carrier does in a physical collocation arrangement.[70] Tr. 690-93. A carrier can also remotely provision services to customers. Tr. 552-53 (Covad). In both physical and virtual collocation arrangements, these functions are performed remotely to avoid the costs associated with dispatching a technician. Tr. 691-92.

Third, with virtual collocation, once the carrier determines that a technician needs to physically work on the equipment to resolve a problem, the carrier would enter a repair ticket into Verizon's system through an interface or by making a telephone call. Tr. 697. After that, however, the ticket is included in nondiscriminatory fashion into the CO workload balance, in which all carrier troubles are treated equally without distinction as to whether it concerns a collocated carrier or Verizon. Work is then assigned appropriate priorities based on the outage condition regardless of who the carrier is. Tr. 699. A

---

[70] Even with physical collocation arrangements, carriers do not always dispatch a technician. Tr. 691. Generally, when an "alarm" is generated on the physically collocated equipment, the alarm indicator would appear remotely at the carrier's remote operations center to alert the carrier that there is a problem. Tr. 695. The carrier would then remotely diagnose the condition to determine whether to dispatch a technician. Tr. 693.

Remote access is comparable to and, in some cases, can be better than "hands-on" access when assessing the condition of the equipment. Tr. 693-94. For example, using a Digital Subscriber Line Access Multiplexer ("DSLAM"), the carrier would connect a remote circuit into the channel bank. The carrier would then access the channel bank remotely to provision or determine the condition of a customer's port. Tr. 691. They could also remotely diagnose trouble conditions in the equipment and test for proper functionality. Tr. 691. The remote access circuit is connected to an interface port. The telemetry port used by the remote center must be unplugged for the on-site technician to connect a lap-top computer. Tr. 693. The result for the carrier is that the remote access circuit is just like being in front of the collocated equipment. Tr. 694.

Verizon CO technician trained to work on the virtually collocated equipment would be dispatched to work on the carrier's virtual arrangement at the direction of the carrier.[71] Tr. 696, 698. Once the Verizon technician is dispatched, this is truly a *collaborative* process.[72] Tr. 88-89.

In a virtual arrangement, the Verizon technician would work with the carrier's monitoring center, if necessary, in much the same way that a Verizon technician would contact the Verizon's monitoring center to repair Verizon equipment. Tr. 696. In addition, with virtual collocation, the carrier has the option to enter the CO with an escort in the event that Tier 2 support is required to restore service. Tr. 62, 707. However, in this case, only the Verizon technician would be permitted to physically work on that equipment under the carrier's direction. Tr. 708. This is prudent since the Verizon technician would be more knowledgeable regarding protecting other network equipment in close proximity to the virtual arrangement. *Id*.

Fourth, contrary to some parties' claims, virtual collocation does not increase the risk of a cyber attack on Verizon MA's network. Tr. 693. Since many network surveillance and diagnostic functions are performed remotely even in a physical collocation arrangement, the potential risk would be the same regardless of the form of collocation. That risk, however, is low, because the carrier's telemetry circuit typically

---

71 Verizon would strive to match the workforce to the workload needs in supporting virtual collocation. Tr. 701-703., Verizon would follow the same processes it uses when assigning work and restoring services to its end-user customers. Tr. 696.

72 On that basis, AT&T's recommendation that performance metrics be established for maintenance on virtual arrangements is infeasible. Exh. ATT 1, at 23; Exh. VZ MA 2, at 19. Because the carrier is such an integral part of the "exchange" between the companies in restoring service under virtual collocation, it would be impossible – and inherently unfair – to measure only Verizon. Moreover, existing performance metrics for "mean time to restore" are circuit-specific (*e.g.*, DS1, versus DS3), and are not based on the type of collocation arrangement. Tr. 298-99.

does not pass through Verizon MA's network for remote access to its equipment. Tr. 693. In addition, Verizon MA has safeguards (*e.g.*, passwords, authentications, etc.) to access its network and prevent cyber attacks. Tr. 693..

Accordingly, requiring virtual collocation under certain circumstances as set forth in Verizon MA's collocation security proposal is reasonable and appropriate from a network security standpoint. Although escorts may be an alternative in such cases, this would not reduce the level of "foot traffic" in Verizon MA's COs, which is the most effective way to address Verizon's – and the Department's - security concerns. Tr. 701, 705, 708.

G. Verizon MA's Collocation Security Proposal Does Not Differ From Those Employed By Other Telecommunications Carriers.

Finally, the parties' claim that Verizon MA' collocation security proposal excessively limits access to Verizon locations is disingenuous. No carrier allows other carriers' personnel unrestricted access to its equipment. In fact, other carriers' security measures are at least as stringent as those Verizon MA proposes here. Tr. 259, Exh. VZ MA 2, at 27. This is based on Verizon MA's firsthand experience with locating equipment on other carriers' premises to deliver entrance facilities primarily for access services in Massachusetts. Tr. 709.

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. Tr. 260; Exh. VZ MA 2, at 27. 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 and escort the Verizon employee. Exh. VZ-MA-1 at 28.

Within the AT&T facility, AT&T usually places Verizon MA's equipment 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. Exh. VZ MA-1, at 28. When third parties must traverse through areas where AT&T equipment is located to reach their own facilities, AT&T generally requires an AT&T employee escort. Tr. 470-71.

Another carrier with facilities in Massachusetts, NEON, recently modified its procedures for access to its location in Worcester. Under the old arrangement, Verizon MA 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 established by NEON following September 11, 2001, requires Verizon to provide 48 hours' notice to obtain escorted access to the facility. Exh. VZ-MA 1 at 29. In light of other carriers' procedures, Verizon MA's current practices and proposed collocation security plan are reasonable, and the Department should endorse them.

IV. CONCLUSION

The Department's objective in this investigation is to ensure proper protection of the network and preserve the telecommunications infrastructure in Massachusetts. Verizon MA's collocation security proposal would establish *pro-active* security

procedures that would secure and segregate – and, therefore, better protect - the telecommunications network infrastructure from harm – both unintentional and deliberate. These are reasonable and necessary security measures, particularly in light of legitimately heightened security concerns resulting from the events of September 11th.

As demonstrated above, restricting "access" to the COs and RTs is the most effective means of ensuring network reliability for its carrier and end-user customers. Contrary to the parties' unsubstantiated claims, Verizon MA's proposal is lawful and non-discriminatory. Moreover, it reduces the risk of harm to facilities and personnel, while allowing for competition. Tr. 42. Verizon MA's proposal would also maintain and enhance existing security procedures, and has minimal effect on existing collocation arrangements. Accordingly, Verizon MA's collocation security proposal is reasonable and should be approved.

Respectfully submitted,

VERIZON MASSACHUSETTS

By its attorneys,

_____

Barbara Anne Sousa
Gregory Kennan
185 Franklin Street, 13th Floor
Boston, Massachusetts 02110-1585
(617) 743-7331
(617) 743-2255

Dated: August 9, 2002