D.T.E. 02-8 May 25, 2005

Investigation by the Department of Telecommunications and Energy on its own motion, pursuant to G.L. c. 159, §§ 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts.

APPEARANCES: Barbara Anne Sousa, Esq.
Gregory M. Kennan, Esq.
Verizon Massachusetts
185 Franklin Street - Room 1403
Boston, MA 02110
Intervenor

Thomas Reilly, Esq.
Attorney General of the Commonwealth of Massachusetts
By: Karlen J. Reed, Esq.
Assistant Attorney General
Office of the Attorney General
Utilities Division
One Ashburton Place
Boston, MA 02108
Intervenor

Robert D. Shapiro, Esq.
Christopher H. Kallaher, Esq.
Rubin and Rudman LLP
50 Rowes Wharf
Boston, MA 02110
FOR: Allegiance Telecom, Inc.
Covad Communications Company

-and-

Mary Albert
Vice President, Regulatory and Interconnection
Allegiance Telecom, Inc.
1919 M Street, NW, Suite 420
Washington, D.C. 20036
Intervenors

Mary E. Burgess, Esq.
Philip S. Shapiro, Esq.
AT&T Communications, Inc.
111 Washington Ave. - Room 706
Albany, NY 12210

-and-

Patricia A. Jacobs, State Director, Law & Government Affairs
Jay E. Gruber, Esq.
AT&T Communications of N.E., Inc.
99 Bedford Street, Suite 420
Boston, MA 02111

-and-

Jeffrey F. Jones, Esq.
Kenneth W. Salinger, Esq.
Palmer & Dodge, LLP
111 Huntington Avenue
Boston, MA 02199-7613
FOR: AT&T Communications of New England, Inc.
Intervenor

Scott Sawyer, Esq.
Vice President-Regulatory Affairs
Conversent Communications of Massachusetts, LLC
222 Richmond Street, Suite 301
Providence, RI 02903
Intervenor

Andrea Pruitt Edmonds, Esq.
Jason Karp, Esq.
Kelley Drye & WarrenLLP
8000 Towers Crescent Drive, Suite 1200
Vienna, VA 22182
FOR: Covad Communications Company

-and-

Anthony Hansel, Esq.
Senior Counsel
Covad Communications Company
600 14th Street, N.W. Suite 750
Washington, D.C. 20005
Intervenor

William J. Rooney, Jr. General Counsel
John O. Postl, Assistant General Counsel
Global NAPs, Inc.
89 Access Road, Suite B
Norwood, MA 02062
Intervenor

Betsy L. Ehrenberg, Esq.
Pyle, Rome, Lichten & Ehrenberg, P.C.
18 Tremont Street, Suite 500
Boston, MA 02108
FOR: International Brotherhood of Electrical Workers, AFL-CIO
Intervenor

Stephen A. Bogiages, Esq.
General Counsel
NEON Optica, Inc.
2200 West Park Drive - Suite 200
Westborough, MA 01580
Intervenor

Kristin L. Smith, Esq.
Qwest Communications Corporation
1801 California Street - Suite 4900
Denver, CO 80202
Intervenor

Craig D. Dingwall, Esq.
Director and General Attorney
Sprint Communications Company L.P.
401 9th Street, NW, Suite 400
Washington, DC 20004
Intervenor

Richard C. Fipphen, Esq.
MCI, Inc.
200 Park Avenue, 6th Floor
New York, NY 10166
Intervenor

Karen Nations, Esq.
Regulatory Director
XO Massachusetts, Inc.
45 Eisenhower Drive, 5th Floor
Paramus, NJ 07652
Intervenor

TABLE OF CONTENTS

I. INTRODUCTION

On January 24, 2002, the Department of Telecommunications and Energy ("Department"), on its own motion, opened an investigation into collocation security in Massachusetts. The investigation was initiated to examine the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts ("Verizon") in light of heightened security concerns after the terrorist attacks on September 11, 2001. Collocation Security Investigation, D.T.E. 02-8, at 1, Vote and Order to Open Investigation (January 24, 2002) ("Order to Open Investigation"). The Department stated that the purpose of its investigation was to review the Department's prior findings with respect to access by personnel of other carriers to Verizon's central offices ("COs") and other facilities, and to assess the security measures in place to protect those facilities. Id. In addition, the Department stated that it intended to determine which policies, if any, should be strengthened to safeguard telecommunications networks from tampering and thereby ensure reliable telecommunications service to the citizens of Massachusetts.[1] Id.

In its Order to Open Investigation, the Department stated that the investigation would determine whether Verizon's security policies meet the statutory standard for "just, reasonable, safe, adequate and proper regulations and practices." Id. at 6-7, citing G.L. c. 159, § 16. The Department specified that the investigation would examine the following issues: (1) the extent and nature of appropriate access by personnel of other carriers to Verizon's COs and other

---

[1] The instant proceeding addresses intentional, as opposed to unintentional, network damage. Order to Open Investigation at 1.

facilities for accessing collocation sites; (2) whether cageless collocation arrangements[2] remain an acceptable security risk; (3) the adequacy of security measures implemented in Verizon's COs and other facilities, focusing on preventive, rather than "after-the-fact," measures; and (4) other related security issues. Id. at 7.

II. PROCEDURAL HISTORY

On February 25, 2002, the Department held a public hearing and procedural conference. At the public hearing, the Department granted the petitions to intervene of Verizon, Allegiance Telecom of Massachusetts, Inc. ("Allegiance"), AT&T Communications of New England, Inc. ("AT&T"), Conversent Communications of Massachusetts, LLC ("Conversent"), Covad Communications Company ("Covad"), Global NAPs, Inc. ("Global NAPs"), International Brotherhood of Electrical Workers ("Union"), NEON Optica, Inc. ("NEON"), Qwest Communications Corporation ("Qwest"), Sprint Communications Company, L.P. ("Sprint"), MCI, Inc. ("MCI," formerly WorldCom), and XO Communications ("XO"). In addition, the Department received a notice of intervention from the Massachusetts Attorney General's Office.

At the procedural conference, the Department established a date for Verizon to file a collocation security report on existing CO security and a proposal for any CO security

---

[2] Cageless collocation ("CCOE") differs from caged collocation, in which termination equipment is placed in a segregated physical space in the CO, and virtual collocation, in which the incumbent local exchange carrier ("ILEC") maintains equipment for competitive local exchange carriers ("CLECs") and access by CLEC personnel is not permitted. See Order to Open Investigation at 2 n.2. CCOE is a type of physical collocation arrangement that allows placement of CLEC equipment in non-secured, non-separated spaces in an ILEC's COs (see Exh. VZ-1, at 10).

changes. On April 5, 2002, Verizon filed panel testimony that included a description of current security measures and a proposal to increase collocation security measures ("Verizon Proposal"). The Department received rebuttal testimony from AT&T, MCI, Sprint, Covad, Allegiance, and Qwest on May 15, 2002. Verizon filed surrebuttal panel testimony on June 18, 2002. The parties conducted extensive discovery.

On April 24, 2002, AT&T, Sprint, Global Naps, Covad, Conversent, and Allegiance filed with the Department a Motion to Suspend Current Litigation Proceedings and to Establish an Industry Task Force on Network Security in Lieu of Divisive Litigation and Request for Expedited Ruling on Motion ("Joint Motion"). In the Joint Motion, the moving parties requested that the Department (1) suspend the current procedural schedule, and (2) establish an industry task force to address security issues at Verizon's COs where carriers' networks are interconnected (Joint Motion at 9-10.) The Hearing Officer requested comment on the Joint Motion on April 24, 2002. Comments were received from Verizon, the Attorney General, MCI, XO, Qwest, and the Union.

In a ruling issued May 6, 2002, the Hearing Officer denied the moving parties' request to suspend the procedural schedule and establish an industry task force. Collocation Security Investigation, D.T.E. 02-8, Hearing Officer Ruling on Joint Motion (May 6, 2002) ("Ruling on Joint Motion"). The Hearing Officer stated that the Department intended this investigation to focus on the issue of collocation security, and that the scope of issues the movants suggested be addressed by the proposed task force was far broader than this particular investigation. Ruling on Joint Motion at 5. The Hearing Officer did note that broader issues of

telecommunications network security were being addressed outside of the Department's D.T.E. 02-8 investigation by the Network Reliability and Interoperability Council ("NRIC")[3] on a national basis, and also by the Department itself in its review of network reliability plans from local exchange carriers operating in Massachusetts.[4]

On May 8, 2002, XO filed a Motion to Compel Verizon Responses to XO Information Requests, and a day later, Allegiance filed a Motion to Compel Responses to Information Requests. In a Hearing Officer Ruling issued June 28, 2002, the Hearing Officer denied the motions to compel, and clarified the role of cost information in this proceeding. Collocation Security Investigation, D.T.E. 02-8, Hearing Officer Ruling on Motions of XO Massachusetts, Inc. and Allegiance Telecom of Massachusetts, Inc. (June 28, 2002) ("Ruling on Motion to

---

[3] The NRIC is a national industry collaborative which identifies areas for improvement to protect the nation's telecommunications networks from natural or man-made incidents. Shortly before the Department opened this investigation in response to "heightened security concerns after the events of September 11, 2001," the NRIC incorporated into its charter a similar objective. Specifically, NRIC focused on the security and reliability of telecommunications networks across the nation to ensure the availability and rapid restoration of telecommunications during periods of "exceptional stress due to natural disaster, terrorist attacks, or similar occurrences." Charter of the Network Reliability and Interoperability Council - VI at B (available at http://www.nric.org/charter_vi/). By March 2003, NRIC identified and submitted for adoption 249 physical security prevention and restoration Best Practices, a carrier mutual aid agreement, and provided recommendations to carriers and public safety officials on ways to work together and ensure better disaster preparedness. See http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-232180A2.pdf.

[4] See Memorandum to Massachusetts Facilities-Based Telecommunications Service Providers from Michael Isenberg, Director, Telecommunications Division (February 7, 2002) (requiring all facilities-based carriers to submit a Network Reliability and Emergency Response Plan to the Department for review). The plans submitted in response to this memorandum were reviewed by the Department and are retained on file.

Compel"). The Ruling on Motion to Compel stated that in the first portion of the proceeding, the Department would address Verizon's obligations with respect to CO security, and whether Verizon was meeting those obligations; if the Department made a finding that Verizon was not meeting its obligations, then the Department would order Verizon to make certain changes. Ruling on Motion to Compel at 5. The Ruling on Motion to Compel also stated that before adopting specific policies, the Department would require Verizon to submit a filing outlining in detail how it would comply with the Department's directives, and include supporting cost data. Id. The Department would then address the cost-effectiveness of Verizon's proposed security methods at that time. Id.

The Department conducted evidentiary hearings on July 10 – July 12, 2002. Verizon sponsored the panel testimony of Lawrence R. Craft, manager of Verizon security, Francesco S. Mattera, director of network operations, Lynelle Reney, director for collocation for Verizon East, and Peter Shepard, director of state regulatory planning. Allegiance sponsored the testimony of Wendy Perrott, senior manager for collocation systems. AT&T sponsored the testimony of E. Christopher Nurse, district manager of government affairs, Michael S. Paszynsky, director of corporate security and claims, Douglas Gorham, operations manager with AT&T Local Network Services, and Anthony Fea, division manager with AT&T Local Network Systems. MCI sponsored the testimony of Roy Lathrop, economist in the MCI regulatory analysis group. Sprint sponsored the testimony of Edward B. Fox, senior manager for regulatory policy. Covad sponsored the testimony of Michael Clancy, director of government and external affairs, and Bart Shea, senior Engineer, Furnish, and Install

("EF&I") manager. Qwest sponsored the testimony of Anne Cullather, senior director of industry affairs, and Michael Adragna, senior manager of physical security.

Initial Briefs were filed by Verizon, the Attorney General, Allegiance, AT&T, Covad, Qwest, Sprint, and MCI. Reply briefs were filed by Verizon, Allegiance, AT&T, Covad, Qwest, Sprint, MCI, and XO. The evidentiary record consists of 207 exhibits, and responses to 17 record requests.

III. OUTSTANDING PROCEDURAL MOTIONS

A. Introduction and Descriptions of Motions

On May 21, 2002, AT&T filed a Motion for Confidential Treatment ("AT&T Motion") of Attachment No. 1 of its panel rebuttal testimony dated May 15, 2002 (later entered into the evidentiary record as Exh. ATT-1). Attachment No. 1 to Exh. ATT-1 consists of a diagram depicting a method of interconnection at an AT&T collocation site (AT&T Motion at 3). According to AT&T, this method of interconnection was developed by AT&T at its own expense for its own internal purposes, is not publicly available, and is subject to elaborate internal protections (id. at 4). AT&T argues that the information depicted in Attachment No. 1 is of considerable commercial value to AT&T, and that disclosing the information would have an adverse affect on marketing because it reveals the presence of equipment that provides certain services, allowing competitors to target certain services provided to local exchange customers (id. at 4-5). AT&T asks that the Department protect the information in Attachment No. 1 for five years (id. at 5). No party objected to AT&T's Motion.

Verizon filed motions for confidential treatment on June 27, 2002 ("Verizon June Motion") and on July 26, 2002 ("Verizon July Motion"). In its June Motion, Verizon seeks confidential treatment for its response to Allegiance information request number AL-VZ-2-1, parts (e) and (h), entered into the evidentiary record as Exh. AL-VZ-2-1. According to Verizon, part (e) of Exh. AL-VZ-2-1 contains internal security methods and procedures, and part (h) contains the results of internal security reviews on a CO-specific basis (see Verizon June Motion at 3). Verizon argues that part (e) is a blueprint of its internal security practices that, if made public, could pose a significant security risk for Verizon's facilities, equipment and personnel (id. at 4). Verizon cites to other proceedings in which the Department has granted confidential treatment to internal methods and procedures (id.). Verizon also argues that part (h) contains the results of internal security inspection reports for approximately 160 COs, and includes detailed information regarding security measures used at each site (id.). According to Verizon, public access to this information would undermine Verizon's security efforts and enable potential perpetrators to target certain COs based on Verizon's security profile (id. at 5).

In Verizon's July Motion, Verizon asks for confidential treatment of its response to record request IBEW-VZ-1, which contains an alphabetical list of Massachusetts COs that Verizon considers "network-critical sites"[5] (Verizon July Motion at 3). According to Verizon, this information is held in the strictest confidence by only a few employees, and is highly

---

[5] According to Verizon, "network-critical sites" are those Verizon COs necessary for the "survivability of Verizon MA's network" (Verizon July Motion at 3).

sensitive, proprietary information from a network, security, and commercial perspective (id.). Verizon further asks that the Department restrict access to this information to the Department only (id.). Verizon argues that the restriction is necessary because of the serious consequences that would occur if this data were made available, and that a standard protective agreement would not adequately protect the data (id. at 3-4). Finally, Verizon contends that its request is valid because the data requested is not relevant to this proceeding, and therefore there is no compelling need to provide the list to parties in this proceeding (id. at 4). No party objected to either Verizon's June or July Motions.

B. Standard of Review for Motions for Confidential Treatment

Information filed with the Department may be protected from public disclosure pursuant to G.L. c. 25, § 5D, which states in part that:

> The [D]epartment may protect from public disclosure, trade secrets, confidential, competitively sensitive or other proprietary information provided in the course of proceedings conducted pursuant to this chapter. There shall be a presumption that the information for which such protection is sought is public information and the burden shall be upon the proponent of such protection to prove the need for such protection. Where such a need has been found to exist, the Department shall protect only so much of the information as is necessary to meet such need.

G.L. c. 25, § 5D permits the Department, in certain narrowly defined circumstances, to grant exemptions from the general statutory mandate that all documents and data received by an agency of the Commonwealth are to be viewed as public records and, therefore, are to be made available for public review. See G.L. c. 66, § 10; G.L. c. 4, § 7, cl. twenty-sixth. Specifically, G.L. c. 25, § 5D, is an exemption recognized by G.L. c. 4, § 7, cl. twenty-sixth (a) ("specifically or by necessary implication exempted from disclosure by statute").

G.L. c. 25, § 5D establishes a three-part standard for determining whether, and to what extent, information filed by a party in the course of a Department proceeding may be protected from public disclosure. First, the information for which protection is sought must constitute "trade secrets, confidential, competitively sensitive or other proprietary information;" second, the party seeking protection must overcome the G.L. c. 66, § 10, statutory presumption that all such information is public information by "proving" the need for its non-disclosure; and third, even where a party proves such need, the Department may protect only so much of that information as is necessary to meet the established need and may limit the term or length of time such protection will be in effect. See G.L. c. 25, § 5D.

Previous Department applications of the standard set forth in G.L. c. 25, § 5D reflect the narrow scope of this exemption. See Boston Edison Company: Private Fuel Storage Limited Liability Corporation, D.P.U. 96-113, at 4, Hearing Officer Ruling (March 18, 1997) (exemption denied with respect to the terms and conditions of the requesting party's Limited Liability Company Agreement, notwithstanding requesting party's assertion that such terms were competitively sensitive); see also, Standard of Review for Electric Contracts, D.P.U. 96-39, at 2, Letter Order (August 30, 1996) (Department will grant exemption for electricity contract prices, but "[p]roponents will face a more difficult task of overcoming the statutory presumption against the disclosure of other [contract] terms, such as the identity of the customer"); Colonial Gas Company, D.P.U. 96-18, at 4 (1996) (all requests for exemption of terms and conditions of gas supply contracts from public disclosure denied, except for those terms pertaining to pricing).

All parties are reminded that requests for protective treatment have not and will not be granted automatically by the Department. A party's willingness to enter into a non-disclosure agreement with other parties does not resolve the question of whether the response, once it becomes a public record in one of our proceedings, should be granted protective treatment. In short, what parties may agree to share and the terms of that sharing are not dispositive of the Department's scope of action under G.L. c. 25, § 5D, or c. 66, § 10. See Boston Edison Company, D.T.E. 97-95, Interlocutory Order on (1) Motion for Order on Burden of Proof, (2) Proposed Nondisclosure Agreement, and (3) Requests for Protective Treatment (July 2, 1998).

C. Analysis and Rulings

Regarding AT&T's Motion, the diagram at issue in Exh. ATT-1 identifies a mode of collocation that details types of equipment and connections between the equipment. AT&T states that the identity of the equipment reveals the types of service to be provided by this collocation arrangement, and therefore reveals AT&T's marketing plans. AT&T states that, with this knowledge, competitors can target those services with competitive offerings of their own, and therefore gain an unfair competitive advantage. The Department has granted confidential treatment to details of a company's installed lines where disclosure of that information would allow competitors to target unfairly their sales efforts. See Verizon Alternative Regulatory Plan, D.T.E. 01-31-Phase I, at 9, Interlocutory Order (August 29, 2001). In addition, the Department has previously protected network configuration data. See Unbundled Network Elements, D.T.E. 01-20, at 10, Hearing Officers'

Ruling on Motions for Confidential Treatment (December 21, 2001) (granting confidential treatment to details regarding the location, configuration and cost of investments for Verizon's network and granting confidential treatment to detailed information regarding Verizon's feeder and distribution network). The Department finds that the information contained in AT&T's diagram is similar to network information protected above, and, therefore, grants AT&T's Motion.

Regarding Verizon's June Motion, the Department previously has protected carriers' internal methods and procedures. See MediaOne/Bell Atlantic Arbitration, D.T.E. 99-42/43, 99-52, at 51 (2000); Tel-Save, Inc., D.T.E. 98-59, Hearing Officer Ruling (October 22, 1998). The Department determines that Verizon's request for confidential treatment of its internal methods and procedures contained in Exh. AL-VZ-2-1 likewise falls within the Department's standard for confidential treatment, and, therefore, grants Verizon's June Motion relating to internal methods and procedures. Turning to the portion of Exh. AL-VZ-2-1 containing security data, we determine that information that may jeopardize network security by its release falls within the definition of "confidential" information that may be protected by the Department under G.L. c. 25, § 5D. The Massachusetts Public Records Law also recognizes the need to protect certain security and infrastructure information. See G.L. c. 4, § 7, cl. 26(n) (exempting records relating to security of certain infrastructure located within the commonwealth from the sunshine requirements of the Public Records Law). Verizon has requested protection of the results of its internal security reviews, and, therefore, consistent with G.L. c. 25, § 5D and the Public Records Law Exemption noted

above, Department also grants Verizon's June Motion restricting public disclosure of this security data.

Finally, in its July Motion, Verizon seeks expanded protection for its list of network-critical COs contained in RR-IBEW-VZ-1. In addition to shielding this information from the public, Verizon also asks that the Department deny access to the parties in this matter. Under usual circumstances, the Department will require a proponent of confidential information to disclose such information to parties in a Department proceeding with a non-disclosure agreement. The reason for this policy is to prevent a proponent of confidential treatment from prejudicing the due process rights of any party in the proceeding by withholding information necessary for the party to participate in the proceeding. However, in this case, no party objected to Verizon's request to shield this information from the parties, and it is apparent that the parties did not see a need for this information to present their cases. Moreover, as the Department did not rely on the information contained in RR-IBEW-VZ-1 in reaching any of its conclusions in this Order, the Department sees no reason to retain this highly sensitive information and will return the information to Verizon upon release of this Order. Therefore, because we determine there is no need for the Department to retain this information, there is also no need for the Department to rule on this portion of Verizon's July Motion.

IV. STANDARD OF REVIEW

The Department opened its investigation of Verizon's collocation security policies pursuant to G.L. c. 159, §§ 12 and 16. Under § 16, the Department must:

> (1) determine whether [Verizon's] regulations, practices, equipment, or service do not meet the statutory requirement for just, reasonable, safe, proper, and adequate service; and
>
> (2) consider the cost of the remedy and its impact on [Verizon's] financial ability to provide service to the public.

Therefore, the Department will determine whether Verizon's current security policies are, in the words of our standard, just, reasonable, safe, proper, and adequate. If the Department determines that Verizon's current security policies do not comply with our standard, it may order Verizon to change those security policies. To define appropriate changes to Verizon's collocation security policies, if necessary, the Department will take into consideration Verizon's Proposal. Under the Telecommunications Act of 1996 ("Act") and Federal Communications Commission ("FCC") rules, Verizon's collocation security measures must be reasonable. See 47 C.F.R. § 51.323(i). Verizon bears the burden of showing the reasonableness of its existing collocation security policies, and any proposed changes to those policies.

The Act requires that an ILEC provide for physical collocation of equipment necessary for interconnection or access to unbundled network elements at its premises to competitive carriers. 47 U.S.C. § 251(c)(6). The FCC has promulgated regulations to implement the Act's collocation requirements, including regulations addressing issues relating to collocation security. 47 C.F.R. § 51.323. Certain of the FCC's regulations have been subject to court

challenges, and have been revised as a result. See Order to Open Investigation at 3-5, for a history of the FCC's collocation security rules.[6]

The FCC's current rules on collocation appear at 47 C.F.R. § 51.323. The regulations allow ILECs to implement "reasonable security arrangements" to protect their equipment and ensure network reliability, with certain safeguards to protect the rights of collocating parties. 47 C.F.R. § 51.323(i). For example, the ILEC must allow collocating parties access to collocated equipment 24 hours per day, seven days per week, without either requiring a security escort or delaying a competitor's entry into the ILEC's premises. Id. Regarding costs, the FCC's regulations allow an ILEC to require a collocating carrier to pay only for the least expensive, effective security option that is viable for the physical collocation space assigned. Id. The FCC requires that if an ILEC restricts physical collocation to a separate space segregated from ILEC facilities, the ILEC must satisfy five conditions.[7] 47 C.F.R. § 51.323(i)(4). The FCC also imposes parity requirements when an ILEC requires a separate entrance for collocating carriers. 47 C.F.R. § 51.323(i)(5). Finally, the FCC rules

---

[6] Subsequent to the opening of this investigation, the United States Court of Appeals for the District of Columbia Circuit denied petitions for review of the FCC's In the Matter of Deployment of Wireline Services Offering Advanced Telecommunications Capability, CC Docket No. 98-147, Fourth Report and Order, FCC 01-204 (rel. August 8, 2001) ("Collocation Remand Order"), and affirmed the FCC's space allocation rules. Verizon v. FCC, 292 F.3d 903 (D.C. Cir. 2002).

[7] The five required conditions are as follows: (1) legitimate security concerns or operational constraints warrant such separation; (2) affiliate or subsidiary collocation space is also separated; (3) separate space is available in the same time frame as non-separated space; (4) cost of separate space is not materially higher than non-separated space; and (5) separated space is comparable from a technical and engineering standpoint as non-separated space. 47 C.F.R. § 51.323(i)(4).

require that an ILEC assign collocation space to requesting carriers in a just, reasonable, and nondiscriminatory manner, and forbid space assignment practices that negatively affect a collocator's operations by materially increasing costs, materially delaying occupation, impairing quality of service, or unreasonably reducing space available for physical collocation. 47 C.F.R. § 51.323(f)(7).

The Department has also issued Orders addressing collocation security issues. See Order to Open Investigation at 2-5, for a summary of collocation requirements imposed by the Department. Subsequent to hearings in this proceeding, the Department issued an Order in a separate proceeding, D.T.E. 03-29, approving additional Verizon collocation security requirements. In response to a challenge to Verizon's requirement of background checks and drug tests for CLEC employees, the Department found that Verizon's requirements complied with FCC rules and concluded that the requirements are "reasonable security measure[s] that Verizon may adopt to safeguard its equipment and ensure network reliability." Collocation Access Cards, D.T.E. 03-29, at 16 (2003). In that Order, the Department endorsed Verizon's access requirements and determined that (1) Verizon applies its access requirements non-discriminately in that Verizon's employees and contractors are subject to the same requirements for access credentials; (2) the access requirements comply with federal and state laws; (3) the requirements do not violate CLEC employees' right to privacy; and (4) the requirements do not constitute a barrier to entry. Id. at 17-20.

In addition, in other Department proceedings, the Department has required Verizon to demonstrate that proposed security measures are justified. In Verizon Tariffs Nos. 14 and 17,

D.T.E. 98-57, Phase I, at 15-16, Order on Motions for Reconsideration and Clarification (September 7, 2000), the Department stated that "should a CLEC challenge Verizon's decision to deploy multiple security measures in a particular central office or locations of central offices, Verizon has the burden to show that the additional security measures provide a necessary security benefit to justify added costs imposed on CLECs." The Department reiterated this requirement when it required Verizon to add language to tariff D.T.E. MA No. 17 stating that "the Telephone Company has the burden to show that any additional security measures provide a necessary security benefit to justify added costs imposed on the CLEC." D.T.E. 98-57, Phase I-B at 56-57 (May 24, 2001). See also 47 U.S.C. § 251(c)(6) (ILEC must prove to state commission where physical collocation not practical due to technical reasons or because of space limitations); 47 C.F.R. § 51.321(d) (ILEC denying particular method of interconnection or access to unbundled network elements must prove to state commission that requested method is not technically feasible).

V. DESCRIPTION OF VERIZON'S EXISTING SECURITY POLICIES AND VERIZON'S PROPOSAL

Currently, Verizon uses the following security measures to protect its telecommunications infrastructure: (1) collocator identification ("ID") badges; (2) card reader access systems ("CRAS")[8]; (3) key controlled access systems; (4) directional signage and floor markings (e.g., floor tape); (5) manned entrances; and (6) security cameras (Exh. VZ-1, at 17).

---

[8] Verizon deploys CRAS to secure both the exterior walls and interior partitioned spaces of its COs (Exh. AL-VZ-1-1, Att. 2, at 7).

Under Verizon's current security policies, all CLEC employees are required to wear and display their ID badges while on Verizon's premises (id. at Att. 1). CLEC badges may not be loaned or shared, and lost or stolen ID badges must be reported immediately to Verizon (id.). CRAS cards are also issued to individual CLEC employees and are used in conjunction with a Verizon-issued ID badge (id.). CRAS cards allow access only to specific areas of Verizon's premises and may not be loaned or borrowed (id.). Like the ID badges, CRAS cards must be returned to Verizon when the CLEC employee no longer has authorized access to a particular CO (id.). In addition, Verizon issues keys to CLEC management to access locked doors, but prohibits key duplication (id.). Keys must be returned to Verizon when access is no longer valid (id.). Finally, security cameras or closed circuit television cameras ("CCTV") may be used where CLECs have unsecured CCOE arrangements, or where CLECs pass through Verizon's space in the CO (id.).[9]

Verizon's Proposal for additional security measures consists of the following provisions: (1) requiring separate and secured collocation areas (e.g., separate rooms, floors, entrances and/or pathways) for all types of physical collocation arrangements to secure and segregate collocators' equipment from Verizon's network facilities, or virtual arrangements where such space cannot be provisioned; (2) relocating existing unsecured CCOE arrangements to separate and secured space only, or converting CCOE to virtual collocation and closing off the CO entirely to all forms of physical collocation when separate space cannot be provisioned;

---

[9] Verizon's current collocation security measures are also described in VZ Collocation Security Guidelines on its website, http://www.verizon.com/wholesale/clecsupport/east/wholesale/html/pdfs/CollocationSecurityGuidelines-May_02.pdf .

(3) restricting carrier access to shared facilities (e.g., temporary staging areas, loading docks, restrooms, and elevators) that can be separated and secured from Verizon's equipment areas; (4) requiring virtual collocation arrangements only at remote terminals ("RTs"),[10] or imposing an escort requirement for carriers; and (5) converting existing physical collocation arrangements to virtual collocation in COs that have the highest security risk (e.g., COs with certain types of switches, the presence of critical customers, or a high number of access lines) (Exhs. VZ-1, at 23-24, 34, 39-40; VZ-2, at 7).

VI. POSITIONS OF THE PARTIES

A. Verizon

Verizon states that its Proposal provides an appropriate level of network security for collocated COs and RTs in Massachusetts by restricting "foot traffic" in areas where Verizon's facilities and equipment are located (Verizon Brief at 14). Limiting access in its COs and RTs is necessary, according to Verizon, because inadvertent or intentional damage to the critical facilities housed within a CO may potentially cause significant service-affecting consequences, including but not limited to the interruption of public safety or emergency services (id. at 16). Verizon argues that the increase in "foot traffic" due to multiple carriers physically collocating their equipment compromises its ability to secure the network from within its COs (id. at 17). Therefore, Verizon argues that by restricting access to its COs, as well as requiring virtual

---

[10] Remote terminals are freestanding structures (e.g., controlled equipment vaults, huts or cabinets) located outside the CO that house telecommunications equipment (Exh. VZ-1, at 36).

collocation arrangements in certain circumstances, it will be able to reduce the risk of network harm and outages for customers served by those facilities (id. at 20).

To support its argument, Verizon refers to incident reports of security breaches from its Collocation Care Center and Corporate Security Department, dated January 2000 to April 2002, for Verizon inside and outside of Massachusetts (id. at 20-21). These reports, according to Verizon, give some insight into the types of security breaches that occur with increased foot traffic within its COs and the harm or damage that can result to Verizon's and/or collocators' equipment or facilities (id. at 22). Verizon argues that the potential consequences from experienced security breaches reported are far-reaching and warrant adoption of its Proposal (id. at 23).

Verizon argues that its Proposal is reasonable, appropriate, preventive, and addresses issues raised in the Department's investigation (id. at 23-24). Verizon argues that its Proposal is designed to have a minimal impact on existing collocators because it is a continuation of its present collocation security policies, except for the "critical office" component (id. at 15). In particular, Verizon states that it currently locates all types of physical collocation arrangements in separate and secured space in the CO where possible (id. at 24). In addition, Verizon states that with its proposal to locate all cageless collocation arrangements in separate and secured spaces, only one cageless collocation arrangement would have to be converted to virtual collocation (id. at 31). Verizon maintains that its current practices include separate entrances and/or separate pathways to collocation areas, and reasonable access to shared facilities (id. at 33, 36). Verizon also points out that its proposal to prohibit physical collocation at RTs will

not affect the CLECs because no CLECs are currently collocating at RTs in Massachusetts (id. at 38). Finally, Verizon maintains that although it may recover the costs of its Proposal from CLECs, the actual cost to CLECs would be minimal (Verizon Reply Brief at 8). Verizon concludes that its Proposal is not anti-competitive because increased network security benefits all carriers, and the immediate impact on other carriers will be minimal (Verizon Brief at 11).

Verizon states that each aspect of its Proposal is consistent with applicable state and federal law (id. at 24). According to Verizon, FCC rules allow Verizon to adopt "reasonable security measures" for its collocation arrangements, including requiring separate space for physical collocation arrangements and separate entrances under certain circumstances (id. at 11-12, citing 47 C.F.R. § 51.323(i)). Verizon states that it has met the criteria set by the FCC for implementing its proposed restrictions (Verizon Reply Brief at 8). Verizon also contends that it may provide virtual collocation only where it can prove that physical collocation is not "technically feasible," and a determination of technical feasibility must consider security and network reliability factors (Verizon Brief at 12-13, citing 47 U.S.C. § 251(c)(6)). Verizon also argues that its Proposal is generally consistent with the Department's Order in D.T.E. 98-57, Phase I, where Verizon states the Department recognized the need to limit carrier access within COs and enable Verizon to preserve and protect the network infrastructure (id. at 14).

According to Verizon, enhancements to existing security measures alone will not prevent damage to its network and therefore will not ensure network security (id. at 43). While Verizon is upgrading some of its current security measures, such as enhancing personnel

pre-screening before issuance of ID badges or access cards, and expanding the deployment of CRAS, Verizon insists that this alone will not deter or prevent intentional or unintentional damage to its network, which could be substantial and far-reaching (id.). Verizon maintains that the only way to prevent network harm is reduce the level of CLEC "foot traffic" and to secure and segregate CLECs' equipment from Verizon's equipment as described in its Proposal (id. at 58, 60). Verizon argues that adopting its Proposal is a reasonable and necessary measure to ensure network reliability for carriers and end-user customers (id. at 60). Moreover, Verizon argues its Proposal is lawful, non-discriminatory, allows for competition, and, therefore, should be approved (id.).

B. Attorney General

The Attorney General argues that Verizon's current collocation security procedures and requirements are adequate (Attorney General Brief at 4). The Attorney General argues that Verizon's current procedures and requirements allow Verizon to control unauthorized CLEC and non-employee access by using CCTV, requiring employees and non-employees to use ID badges and/or key-controlled or card readers on CO premises, and requiring separate entrances (id.). The Attorney General states that Verizon has acknowledged that it has not experienced any harmful security violations in Massachusetts (id., citing Exh. VZ-1, at 21).

The Attorney General further argues that Verizon should complete a full CO "risk assessment"[11] for all of its Massachusetts COs (id. at 5). The Attorney General argues that

---

[11] According to Verizon, a "risk assessment" is "an assessment of . . . a facility, to determine what the probability is of that facility being at risk from a potential source," (continued…)

Verizon has begun risk assessments for certain "vital" Massachusetts COs, but not for all COs in the Commonwealth (id., citing Tr. 2, at 319, 323). According to the Attorney General, the Department should evaluate the collocation security issue again after such a study has been completed to determine whether additional security measures are required (id.).

The Attorney General contends that Verizon should increase its law enforcement communication efforts to ensure the integrity of its network (id.). The Attorney General argues that the Department should require Verizon to maintain an identical, streamlined policy for both non-employees and employees to give a more accurate view of suspicious activity within the CO (id. at 6). The Attorney General argues that although Verizon's law enforcement referral policy indicates that Verizon always refers suspected violations by non-employees to law enforcement, Verizon actually uses a discretionary process to filter some, but not all, suspected unlawful acts to law enforcement (id. at 5-6, citing Exh. AG-VZ-2-1 (Verizon's Referral to Law Enforcement Policy, and Related Security Practices)). The Attorney General argues that Verizon fails to take advantage of an opportunity to deter unlawful activity by not informing its employees or CLEC collocators of its law enforcement referral policy (id. at 6, citing Tr. 2, at 308-309). The Attorney General further argues that Verizon's failure to take any remedial measures or make any "site hardening" changes after

---

[11](…continued)
and is typically done on a location by location basis (Tr. 1, at 23-24). When a risk assessment is conducted, the type of security deployed is determined by comparing the identified risks in the assessment to the costs associated with preventing them (id. at 24-25).

repeated incidents of theft in the Revere, Massachusetts CO[12] raises questions about Verizon's current efforts to address security concerns (id., citing Tr. 3, at 688).

In response to Verizon's Proposal to designate some Massachusetts COs as "critical" and restrict CLEC access to virtual collocation arrangements only, the Attorney General contends that Verizon has not demonstrated sufficient need at this point to implement these additional collocation security proposals (id. at 7). In support, the Attorney General emphasizes that fewer than 30 reports out of nearly 35,000 Verizon East CLEC collocation incident reports[13] between January 2000 and April 2002, were classified as security-related, and in Massachusetts, none of the incidents resulted in customer service interruptions (id.; see Attorney General Brief at 4, citing RR-DTE-VZ-2; Tr.3, at 626-627, 644-645, 749-753; Exh. AG-VZ-1-1). The Attorney General further states that of the 89 customer service interruption reports Verizon filed with the Department between January 26, 1999 and July 15, 2002,[14] none appeared to involve collocation activities (Attorney General Brief at 7, citing RR-DTE-VZ-3).

---

[12] Sprint reported the theft of a router from the Revere, Massachusetts CO in July 2000, and a router was also reported missing from the same CO in October 2000 (RR-Sprint-VZ-1).

[13] In response to an information request from the Attorney General, Verizon provided reports of security violations involving collocation or collocators reported to its Collocation Care Center and its Corporate Security Department for the Verizon East footprint (Exh. AG-VZ-1-1).

[14] Verizon's response to RR-DTE-VZ-3 includes major service outage notification reports filed with the Department in compliance with the Department's Orders in D.P.U. 89-300, D.P.U. 92-100, and D.T.E. 96-30.

The Attorney General concedes, however, that if circumstances change, Verizon should ask the Department to review this matter again (id. at 8).

C. CLECs[15]

The CLECs argue that Verizon has failed to provide sufficient reliable evidence to prove its Proposal is necessary and will increase collocation security (Sprint Brief at 4-11; Covad Brief at 2, 10-18; Qwest Brief at 3-9; MCI Reply Brief at 6; AT&T Brief at 16; Allegiance Brief at 19, 29; XO Reply Brief at 1, 4). According to the CLECs, Verizon relies on the assumption that a reduction in foot traffic will improve security within its COs, an assumption that the CLECs argue is completely unproven (MCI Brief at 13; Allegiance Brief at 8-11, 20; Qwest Reply Brief at 20; XO Reply Brief at 2; Sprint Reply Brief at 6-7; Covad Brief at 16). The CLECs state the record shows that not one security breach in Verizon's Massachusetts COs was the result of a CLEC employee or that CLEC employees are more likely than Verizon employees to engage in network-affecting incidents (MCI Brief at 11-12; Covad Brief at 6, 16; Allegiance Brief at 2, 6-7; Sprint Brief at 9; XO Reply Brief at 3). Allegiance dismisses Verizon's claim by pointing out that although the increasing number of collocation arrangements between 1992 and 2000 led to increasing CLEC foot traffic, the number of network-affecting incidents involving CLECs in Massachusetts remained at zero (Allegiance Brief at 8-11). Finally, the CLECs argue that Verizon has crafted its Proposal without conducting an in-depth risk assessment at any of its Massachusetts COs (AT&T Brief

---

[15] Because their positions are similar, in this section we summarize the positions of AT&T, MCI, Covad, Allegiance, Sprint, Qwest, and XO.

at 12; MCI Brief at 11; Allegiance Brief at 6; Qwest Brief at 7; Sprint Brief at 6). The CLECs contend that Verizon has failed to provide the necessary information to support the reasonableness of its Proposal, thus giving the Department no basis to adopt Verizon's Proposal (MCI Brief at 10-13; Allegiance Brief at 2; Qwest Brief at 11).

Not only do the CLECs argue that Verizon has failed to support its Proposal, but also that Verizon's Proposal is unlawful under both federal and state law (Covad Brief at 12; Qwest Brief at 12; Allegiance Brief at 12-13; Sprint Brief at 23-30). The CLECs argue that Verizon's "separate and secured only" proposal violates the FCC's Collocation Remand Order, which establishes specific criteria for the limited circumstances when segregation of collocators' equipment is allowed (Covad Brief at 12; Qwest Brief at 12; Allegiance Brief at 12-13; Sprint Brief at 23-30). The CLECs also contend that Verizon's "separate and secured only" policy will lead to premature space exhaust, in violation of 47 C.F.R. § 51.323(f)(7), which requires ILECs to assign collocation space to requesting carriers in a just, reasonable, and nondiscriminatory manner, and prohibits ILEC space assignment policies from unreasonably reducing the total space available for physical collocation (Qwest Brief at 14; Covad Reply Brief at 3). Additionally, the CLECs contend that the elimination of physical collocation through Verizon's "virtual collocation only" proposal violates Section 251(c)(6) of the Act and the FCC's Advanced Services Order,[16] which permits CLECs

---

[16] In the Matter of Deployment of Wireline Services Offering Advanced Telecommunications Capability, CC Docket 98-147 et al., First Report and Order and Further Notice of Proposed Rulemaking, FCC 99-48 (rel. March 31, 1999) ("Advanced Services Order").

to have around-the-clock access to their equipment (MCI Brief at 8; Covad Brief at 15; Qwest Brief at 16-17; Sprint Brief at 16-17). Furthermore, the CLECs state that for them to bear the cost of implementation violates federal regulation where collocators are required to pay only for the least-cost, effective security option that is viable for a particular physical collocation space (MCI Brief at 8, quoting 47 C.F.R. § 51.323(i); Qwest Brief at 13; Sprint Brief at 13-14). The CLECs also argue that Verizon presents no cost studies to justify its costly Proposal (Sprint Brief at 15-16; Covad Brief at 18; XO Reply Brief at 1-2; MCI Brief at 8).

The CLECs further argue that elements of Verizon's Proposal are anti-competitive because the Proposal seeks to eliminate CLEC access to Verizon's COs (MCI Brief at 9; Covad Brief at 10-12; Allegiance Brief at 20; Qwest Brief at 11; XO Reply Brief at 1). Verizon's "virtual collocation only" proposal, according to the CLECs, severely limits CLECs' ability to meet the needs of their customers and to distinguish their services from Verizon's because they would be entirely dependent upon Verizon for maintenance and repairs (Qwest Brief at 17-18; Covad Brief at 3-4, 16; Allegiance Brief at 26-28; MCI Brief at 4, 10; Sprint Brief at 31).[17] In addition, CLECs argue that Verizon failed to meet its burden of proof

---

[17] The CLECs argue unanimously that virtual collocation is inferior to physical collocation, and, thus, it is "not a viable alternative" (Allegiance Brief at 26-27; see also Covad Brief at 3-5; AT&T Brief at 20-23). According to the CLECs, virtual collocation arrangements prevent CLECs from controlling their own equipment and network service offerings, which can result in delays for network growth and render an inability to meet customer needs in a timely manner (AT&T Brief at 17; Qwest Brief at 17-18; Covad Brief at 3-5; Allegiance Brief at 26-28). Moreover, Covad states that in Massachusetts there are 950 physical collocation arrangements compared to only three virtual collocation arrangements (Covad Reply Brief at 7). Although it currently has virtual collocation arrangements, Covad states that as a result of its negative

(continued…)

to refuse physical collocation (MCI Brief at 10; AT&T Reply Brief at 18-19; Sprint Reply Brief at 13). The CLECs argue that Verizon's "separate and secured only" proposal and its classification of certain COs as "critical" will force CLECs to accept either virtual collocation arrangements or not to serve customers out of those COs (Qwest Brief at 15; Covad Brief at 5). The CLECs argue that eliminating physical collocation from any of Verizon's COs is discriminatory and will impede competition in Massachusetts (Allegiance Brief at 25-26; MCI Brief at 10; Qwest Brief at 16; XO Reply Brief at 1; Sprint Brief at 35; Covad Brief at 3, 5; AT&T Brief at 16-18).

Allegiance contends that under state law, the Department must make a finding that Verizon's practices are unjust or unreasonable, which the Department has not done, before it can proceed to a determination of which just and reasonable practices are to be put into place (Allegiance Reply Brief at 1-3, citing G.L. c. 159, § 16). In addition, Sprint argues that Verizon's Proposal violates G.L. c. 159, § 16, as well as the Department's collocation orders, Verizon's Tariff No. 17, and Sprint's interconnection agreement with Verizon (Sprint Brief at 2, 7, 34-35).

Also, several CLECs argue that Verizon's current security measures are adequate, but could be enhanced without resorting to the drastic changes that Verizon has proposed (Covad Brief at 6-7; Allegiance Brief at 4-8; AT&T Brief at 34-40). Several argue that a full risk assessment of each CO is required to fully identify the current adequacy of Verizon's

---

[17](…continued)
experience with Verizon, it is in the process of converting its virtual arrangements to physical arrangements (Covad Brief at 3).

collocation security (AT&T Brief at 12-13; Qwest Brief at 7-8; Covad Brief at 7-10). The CLECs provide several alternative recommendations for the Department to consider should it choose to modify Verizon's CO security in Massachusetts. One recommendation is for the Department to ensure that Verizon enforces existing CO security measures properly prior to adopting any new security measures and for the Department to direct carriers to employ the guidelines adopted by the national government and industry groups participating in the NRIC (Qwest Brief at 19-20, 24-25; Sprint Brief at 10-12). Some CLECs argue that Verizon should improve its communications with CLECs (AT&T Brief at 36; MCI Reply Brief at 7); improve its background checks of CLEC personnel (AT&T Brief at 37-38; Covad Brief at 8); and provide better security for CLEC equipment (Sprint Brief at 12). Alternatively, some CLECs recommend that the Department form an industry task force to evaluate current security issues and to determine necessary, cost-effective, nondiscriminatory improvements to Verizon's existing security measures (Covad Brief at 19; Sprint Brief at 36). Some CLECs urge Verizon to deploy additional electronic security equipment, such as CRAS with an anti-passback[18] feature, and additional CCTV (AT&T Brief at 38-40; Sprint Brief at 12; MCI Reply Brief at 5). Additionally, MCI suggests the Department monitor Verizon's ongoing efforts to bring its current security measures up-to-date (MCI Brief at 15-16).

---

[18] An anti-passback feature prevents an individual who has left a CO without swiping out his access card from reentering that CO or entering any other CO (see Exh. ATT-1, at 14).

VII. ANALYSIS AND FINDINGS

A. Introduction

In response to our Order to Open Investigation, Verizon submitted a description of its current security measures, and a proposal to enhance CO security on the basis that the "influx of [CLEC] 'foot traffic' in the CO dramatically increases the security risks to the network infrastructure" (Exh. VZ-1, at 42). As discussed above in Section IV, Verizon bears the burden to prove the reasonableness of additional collocation security measures, including a showing that additional security measures provide a necessary security benefit to justify the added costs imposed on CLECs. D.T.E. 98-57, Phase I, at 15-16; D.T.E. 98-57, Phase I-B at 56-57. As discussed further below, after reviewing the extensive record in this proceeding, we determine that Verizon has not met the burden of proof required to justify implementation of Verizon's April 5, 2002 Proposal, and that Verizon's current security measures are adequate to protect Verizon and CLEC equipment housed in Verizon's COs. However, we conclude that Verizon must make certain that its current security procedures are rigorously enforced to ensure adequate security. In addition, we conclude that in order to monitor changing security needs, the Department will require Verizon to file reports with the Department which will track security-related incidents and responses.

B. Verizon's Proposal

For the following reasons, we conclude that Verizon has not met the burden of proof required to justify implementation of its April 5, 2002 Proposal. Although Verizon argues that the potential ramifications from a security breach "are far-reaching, and warrant adoption of

Verizon MA's collocation security proposal" (see Verizon Brief at 2-6, 23), the Department finds little evidence to substantiate a finding that Verizon's current security measures are inadequate to prevent network tampering in Verizon's COs. Verizon states that it did not rely upon risk assessments performed on individual COs when making its Proposal, although Verizon agrees that "risk assessments are an important part of a process that leads to the adoption of appropriate security measures for the facility that is being assessed" (Tr. 1, at 198-199). By not relying on risk assessments, Verizon has not demonstrated that specific vulnerabilities exist within its COs that would warrant the adoption of its Proposal, and has not shown how its Proposal would effectively address specific security concerns.

In response to information requests by both the Attorney General and the Department, Verizon provided information regarding CO incident reports from January 2000 - April 2002[19] (Exh. AG-VZ-1-1), and service outage reports from January 1999 - May 2002 (RR-DTE-VZ-3). Because Exh. AG-VZ-1-1 included incident reports from outside of Massachusetts, Verizon separately identified those incidents that occurred within COs in

---

[19] Verizon's generated its incident reports contained Exh. AG-VZ-1-1 from two separate databases: (1) Verizon's Collocation Care Center database; and (2) Verizon's corporate security database (Tr. 2, at 370). However, Verizon's inclusion of security incident reports from these two databases led to an over-counting of the actual number of security incidents involving CLECs or CLEC equipment in Massachusetts, because Verizon included duplicate reports (id. at 372) and reports for incidents outside of Massachusetts in its response (id. at 383). At the same time, Exh. AG-VZ-1-1 results in under-reporting of security incidents in Verizon's Massachusetts COs because Verizon only used the keywords "CLEC" and "collocation" for its search criteria, and, therefore failed to identify any security incident that did not involve a CLEC or collocation arrangement (e.g., a security incident in a Verizon CO in Massachusetts involving a Verizon employee) (id. at 395-398).

Massachusetts in RR-DTE-VZ-2. Of those incidents specific to Massachusetts, none of the reported incidents occurred in any of Verizon's equipment areas of its COs or involved Verizon's equipment[20] (see RR-DTE-VZ-2, Att.). Moreover, Verizon's network outage reports contained in RR-DTE-VZ-3 filed with the FCC and the Department did not show that the reported network outages were the result of a CLEC employee's actions within Verizon's COs; rather, these network-affecting outages were the result of, inter alia, equipment failure, environmental conditions (e.g., water in cables), or failure by Verizon employees and contractors to follow proper procedures (see RR-DTE-VZ-3, Atts. 1, 2).

Moreover, although Verizon argued that increased CLEC foot traffic in COs increases the potential for network-affecting events in its COs (Exh. VZ-2, at 2-3), Verizon did not provide evidence to prove a correlation between increased foot traffic in COs and an increase in security incidents. Verizon submitted data showing the number of collocation arrangements per year for 1992 – 2002 (Exh. Qwest-VZ-1-4), and data showing the number of security incidents from January 2000 – April 2002 (Exh. AG-VZ-1-1; RR-DTE-VZ-2), but this data does not show a correlation between an increase in the number of collocation arrangements and an increase in security incidents. For the time period for which Verizon provided data, there is a decrease in the number of collocation arrangements with a corresponding decrease in security incidents from 2000 – 2001, but a continued decrease in the number of collocation

---

[20] The evidence establishes a small number of incidents involving CLECs or CLEC equipment in Massachusetts during the reporting period. Verizon reported 953 collocation arrangements in 169 COs in Massachusetts (Exh. VZ-1, at 9-10). For the reporting period January 2000 – April 2002, Verizon reported 28 incidents in Massachusetts involving CLECs or CLEC equipment (RR-DTE-VZ-2).

arrangements with an increase in reported security incidents from 2001 – 2002 (Exh. Qwest-VZ-1-4; RR-DTE-VZ-1). In addition, in response to a question of whether there was any information to support a conclusion that CLEC employees are more likely than Verizon employees to engage in conduct that would pose a threat to equipment located in Verizon's COs, Verizon stated that there are no known instances of such conduct in Massachusetts (Exh. AL-VZ-1-25). Also, of the approximately 160 Building Security Inspection Reports submitted in this proceeding as part of Exh. AL-VZ-2-1, none of the reports identified a security vulnerability relating to CLEC presence in a CO.

Moreover, much of Verizon's Proposal consists of mandating separate and secured collocation areas and walkways for CLECs; in those COs where separate and secured areas and walkways cannot be provisioned, Verizon proposes closing that CO to all forms of physical collocation, which, in essence, would prohibit the provisioning of CCOE in that CO[21] (Exhs. VZ-1, at 23-24; VZ-2, at 7). The FCC rules set forth specific situations where it is reasonable for an ILEC to separate collocation equipment from its own equipment. See 47 C.F.R. § 51.323(i)(4) (defining certain conditions an ILEC must meet when restricting

---

[21] The FCC established CCOE as a viable physical collocation arrangement in the Advanced Services Order at ¶ 42 ("Incumbent LECs must allow competitors to collocate in any unused space in the incumbent LEC's premises, without requiring the construction of a room, cage, or similar structure, and without requiring the creation of a separate entrance to the competitor's collocation space"). After a court challenge, the FCC clarified this earlier order on remand by permitting ILECs to require CLECs to collocate in separate spaces and use separate entrances under specific conditions and "where legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries' competitive concerns, warrant them." Collocation Remand Order at ¶ 102.

physical collocation to space separated from space housing the ILEC's equipment); see also, Collocation Remand Order at ¶ 102 (defining situations where ILEC may require separation of collocated equipment from its own equipment); 47 C.F.R. § 51.323(f)(7) (prohibiting space assignment policies and practices that materially increase collocation costs, materially delay occupancy, impair quality of service on collocator's service, or unreasonably reduce total space available for physical collocation). As discussed above, Verizon has not demonstrated a legitimate security concern that would warrant mandating a "separate and secured" policy. Although we stated in our Order to Open Investigation, at 7 n.4, that "[i]f the Department determines that [CCOE] arrangements constitute an unacceptable security risk, we would petition the FCC for an exemption from its rules requiring cageless collocation," Verizon did not demonstrate in this proceeding any security risks directly related to CCOE. Without evidence to justify seeking an exemption from the cageless collocation requirements, the Department will not petition the FCC for such an exemption.

The FCC has made clear that an ILEC may restrict CLEC access to a CO in certain narrow circumstances, which we determine are not evident here. Verizon has not shown that "specific and significant adverse impacts would result from the requested . . . access"[22] in order to justify the restrictions on CLEC access that Verizon proposes. Notwithstanding its testimony, Verizon does not establish on the record in this proceeding that existing CLEC

---

[22] The FCC requires that an ILEC prove with "clear and convincing evidence" that specific and significant adverse impacts would result." In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, CC Docket No. 96-98, First Report and Order, FCC 96-325, at ¶ 203 (rel. August 8, 1996).

access to COs for purposes of collocation, including CCOE, constitutes an unreasonable security risk. Because Verizon has failed to satisfy its burden of proving the necessity for its proposed security measures, and that the proposed measures provide a needed security benefit, the Department does not adopt Verizon's Proposal.[23]

C. Adequacy of Current Security Measures

Based on the extensive record compiled in this proceeding, we conclude that Verizon's current CO security measures are adequate. Verizon deploys a mix of security measures aimed at restricting unauthorized access to its COs. For example, in order to obtain authorized entry into its COs, Verizon requires that all CLEC employees who seek access to Verizon's facilities apply for an ID badge and an access card (Exh. AL-VZ-1-1, Att. 2, at 5-8). In August 2002, Verizon enhanced its collocation ID badge and access card application process by requiring CLEC applicants to undergo background checks and drug testing prior to receiving access credentials (Exh. VZ-1, at 5; Exh. AL-VZ-1-2).[24] Verizon's enhanced collocation ID badge and access card application requirements provide an increased level of security by screening all potential access cardholders to determine if a potential cardholder poses a risk to the facilities, equipment, and personnel of either Verizon or CLECs. Only upon completion of a successful

---

[23] Because the Department declines to adopt Verizon's Proposal, we do not rule on the possible anti-competitive or discriminatory effects of the Proposal argued by the CLECs.

[24] See Collocation Access Cards, D.T.E. 03-29 (2003).

screening may an applicant receive entry authorization in the form of ID badges and access cards.[25]

A further example of a current preventive security measure is Verizon's use of CRAS. To secure both the exterior and interior of its COs from unauthorized access, Verizon uses CRAS and key entry systems. Verizon states that it is in the process of replacing the key entry systems with CRAS in all of its COs in order to enhance security (Tr. 1, at 110). Although Verizon concedes that CRAS on its own, or in combination with CCTV, may deter some individuals from inappropriate or illegal behavior, Verizon asserts that "[i]t's not a proactive [sic] step per se" (Tr. 1, at 110). The Department disagrees, however: CRAS is not only an "after the fact" security measure, but also prevents future security breaches. No single security measure, or combination thereof, can effectively deter inappropriate behavior all of the time. By securing access points into and within its COs, Verizon is taking a preventive step to restrict unauthorized access that could lead to a network-affecting security breach.

As described above, Verizon's current mix of collocation security policies restrict unauthorized access to its COs by screening those seeking to gain access, and by securing both the interior and exterior of the physical plant. Successfully preventing unauthorized access is among the most effective security measures as far as collocation and CLEC personnel access are concerned. The measures seem tailored to achieve that success. Therefore, the Department determines that Verizon's current collocation security measures are just, reasonable, safe, proper, and adequate as required by G.L. c. 159, § 16.

---

[25] Collocation Access Cards, D.T.E. 03-29, at 17 (2003).

D. Enforcement

Although we have determined above that Verizon's current security measures are adequate, it is a truism that these measures will be effective only if they are rigorously enforced. Failure by Verizon and CLEC employees to follow CO security policies threatens the integrity of these measures. During this proceeding, a number of CLECs stated they do not return the collocation identification badges and access cards of terminated employees (Exhs. VZ-AL-1-6; VZ-WCOM-1-11; VZ-ATT-1-25) in accordance with Verizon's Collocation Handbook Security Guidelines (Exh. AL-VZ-1-1, Att. 2, at 6, 8). Moreover, one CLEC indicated that it is unfamiliar with Verizon's practice of issuing collocation access cards when it stated in response to an information request, "Cards . . . permitting access to Verizon-controlled facilities are not issued by Verizon to individual employees; they are issued at the Company level. As such, there would be no need for [a CLEC] to return these items in the event an individual employee were terminated inasmuch as the cards . . . would still be needed for current [CLEC] personnel to access [CLEC] equipment at Verizon-controlled facilities" (Exh. VZ-WCOM-1-11). However, Verizon issues CRAS access cards and collocation identification badges to individual CLEC employees requesting CO access, and Verizon's policy regarding the use of these cards explicitly states that its access cards "will not be borrowed, transferred or otherwise used by anyone other than the CLEC employee to whom it was issued" (Exh. AL-VZ-1-1, Att. 2, at 8 (emphasis in original)). Further, Verizon's Collocation Handbook states, "The CRAS card must be surrendered to [Verizon] Security by the CLEC via the [Wholesale Network Services] contact or [Local Collocation Coordinator]

when it is no longer valid (e.g., termination of employment) or when requested by [Verizon] management" (id.). Verizon also acknowledged that it knows of its own personnel sharing access cards and failing to report lost ID badges and access cards (Exh. Conv-VZ-1-14). This evidence demonstrates unfamiliarity in some quarters with the assignment requirements of access cards, and occasional failure to comply with Verizon's policy on returning unused and reporting lost ID badges and access cards. The evidence emphasizes the need for Verizon and CLECs to pay increased attention to the existing security requirements. As noted by AT&T at the evidentiary hearing, "[n]inety percent . . . of all security failures occur not in the devices, [they] occur[ ] in the line or linkage between the people apex and the procedure-policy apex. The equipment usually works fine. It's the procedures that usually break down, that are not followed" (Tr. 2, at 462-463).

Therefore, to ensure the effectiveness of the security procedures in Verizon's COs, the Department requires all carriers and their personnel accessing these COs to comply with established collocation security policies and procedures. These security procedures must be enforced for both Verizon and CLECs. It is crucial that all personnel entering Verizon's COs abide by the policies and procedures established to protect the equipment and safety of individuals within the CO environment. Only then can the effectiveness of Verizon's existing CO security measures be optimized.

E. Reporting Requirements

In order to inform ourselves regarding changing security needs within Verizon's COs, we will require Verizon to provide the following additional information to the Department.

Currently, Verizon compiles reports of security-related incidents that occur in Verizon COs (see Exh. AG-VZ-1-1; RR-DTE-VZ-2). As a new reporting requirement, the Department will require Verizon to provide the Department with an annual summary of incident reports involving Massachusetts COs. In this annual summary, Verizon shall include the locations of the COs involved; the date of the incidents; descriptions of the incidents; whether local police or other law enforcement agency was called to investigate; whether there have been other security violations at that CO, and if so, the dates of prior incidents. In addition, for COs that prove to have recurring security incidents, Verizon will be required to detail the steps it has taken to improve security at the particular CO to prevent further incidents. This annual summary will assist the Department to monitor security breaches at Verizon's Massachusetts COs, and to determine whether existing security measures are sufficient.

Furthermore, we direct Verizon in cooperation with its collocated carriers to review and, where necessary, revise its procedures for tracking issued CO entry badges and for ensuring the return of such badges at appropriate times and the identification and cancellation of lost badges. The Department will expect Verizon to report the outcome of this effort by December 1, 2005.

VIII. ORDER

Accordingly, after notice, hearing, and due consideration, it is

ORDERED: That Verizon's request to approve its Proposal filed April 5, 2002 is hereby denied; and it is

FURTHER ORDERED: That Verizon comply with the Department reporting requirements contained herein; and it is

FURTHER ORDERED: That all parties shall comply with all directives herein.

By Order of the Department,

_____/s/_____
Paul G. Afonso, Chairman

_____/s/_____
James Connelly, Commissioner

_____/s/_____
W. Robert Keating, Commissioner

_____/s/_____
Judith F. Judson, Commissioner

An appeal as to matters of law from any final decision, order or ruling of the Commission may be taken to the Supreme Judicial Court by an aggrieved party in interest by the filing of a written petition praying that the Order of the Commission be modified or set aside in whole or in part. Such petition for appeal shall be filed with the Secretary of the Commission within twenty days after the date of service of the decision, order or ruling of the Commission, or within such further time as the Commission may allow upon request filed prior to the expiration of the twenty days after the date of service of said decision, order or ruling. Within ten days after such petition has been filed, the appealing party shall enter the appeal in the Supreme Judicial Court sitting in Suffolk County by filing a copy thereof with the Clerk of said Court. G.L. c. 25, § 5.