The Commonwealth of Massachusetts

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

D.T.E. 03-29 July 28, 2003

Complaint of Global NAPs, Inc. Against Verizon New England, Inc. d/b/a Verizon Massachusetts for Denial of Issuance of Collocation Access Cards

---

APPEARANCES:

John O. Postl, Esq.
Assistant General Counsel
Global NAPs, Inc.
89 Access Road, Suite B
Norwood, MA 02062
FOR: GLOBAL NAPS, INC.
Complainant

Barbara Anne Sousa, Esq.
Verizon Massachusetts
Room 1403
185 Franklin Street
Boston, MA 02110
FOR: VERIZON NEW ENGLAND, INC. D/B/A VERIZON MASSACHUSETTS
Respondent

TABLE OF CONTENTS

I. INTRODUCTION AND PROCEDURAL HISTORY

On January 13, 2003, Global NAPs, Inc. ("GNAPs") filed a Complaint with the Department of Telecommunications and Energy ("Department") alleging that Verizon New England, Inc. d/b/a Verizon Massachusetts ("Verizon" or "VZ") wrongfully denied GNAPs the issuance of collocation access cards and identification badges needed to obtain access to GNAPs' equipment located in Verizon's facilities.[1] On January 29, 2003, Verizon filed its Answer, asserting that its requirements for issuance of collocation access cards and identification badges are reasonable, non-discriminatory, and consistent with Federal Communications Commission ("FCC") rules. The Department docketed the matter as D.T.E. 03-29.

On March 25, 2003, the Department held a public hearing and procedural conference in D.T.E. 03-29. There were no requests to intervene. The Department established a procedural schedule consisting of a period for discovery and the filing of initial and reply briefs.[2] The parties' positions are summarized below.

---

[1] In order for competitive local exchange providers ("CLECs") to access their physical collocation arrangements in Verizon's central offices ("COs"), CLEC employees must obtain collocation access cards and identification badges from Verizon. See http://www.verizon.com/wholesale/clecsupport/east/wholesale/html/pdfs/CollocationSecurityGuidelines-May_02.pdf ("VZ Collocation Security Guidelines"). A collocation identification badge includes a picture of the CLEC employee and must be worn at all times while in Verizon's facilities. Id. at 6. Verizon's COs are secured by a keyed entry system, a card reader access system ("CRAS"), or a security guard. Id. at 6-7. For those COs that are secured by a CRAS, an access card is required to gain entry. Id. at 7-8.

[2] The Department hereby moves the responses to the Department's and the parties' information requests into the record of this proceeding.

II. POSITIONS OF THE PARTIES

A. GNAPs

GNAPs objects to the changes that Verizon made in August 2002 to its requirements for issuance of non-employee collocation access cards and identification badges (GNAPs Complaint at ¶¶ 3-21).[3] GNAPs argues that provision of personal information, such as date and place of birth, mother's maiden name, and results of a drug test and criminal background check, is unnecessary, constitutes an intrusion into the privacy of CLEC employees, and achieves no legitimate security interest (GNAPs Brief at 4).[4] In addition, GNAPs asserts that requiring CLECs to undertake criminal background checks and drug testing of their employees constitutes a barrier to entry (id.).

GNAPs states that the FCC has promulgated regulations in the areas of collocation and security that require incumbent local exchange carriers ("ILECs"), such as Verizon, to make infrastructure and collocation facilities available to CLECs on terms and conditions that are just, reasonable, and non-discriminatory (id. at 5-6; citing 47 C.F.R. §§ 59.1, 59.2, 51.321, 51.323). GNAPs argues that these regulations identify "reasonable security measures" that

---

[3] For card issuance under Verizon's pre-August 2002 requirements, a CLEC employee was required to include on his access card application, his name, social security number, date and place of birth, and photo ID (see DTE-GN 2-3, Att.; DTE-GN 2-5; VZ Answer at 1-2). Under Verizon's revised requirements, new CLEC employees and CLEC employees whose badges have expired must provide the same information as well as a certification that a drug test and a criminal background check have taken place (DTE-GN 2-3; VZ Answer at 1, Att. 1). Verizon's revised application also requires the applicant's mother's maiden name or a password (see DTE-GN 2-3).

[4] However, in GNAPs Reply Brief, GNAPs acknowledges that it did provide employees' social security numbers, and dates and places of birth, on Verizon's "old" access card and identification badge application, and GNAPs states that it "would agree (reluctantly) to provide [this] information on an ongoing basis" (GNAPs Reply Brief at 2).

involve ILECs' infrastructure (such as installing security cameras and separating collocated equipment), and that the FCC's regulations are non-intrusive with respect to CLEC employees' privacy rights (id. at 6). GNAPs further argues that the FCC recognized that security measures are based on the precautions that an ILEC may take with respect to their premises, but not the people who are entering those premises (id. at 6). According to GNAPs, Verizon's requirements that CLEC employees undergo invasive measures for purported, but unspecified, security reasons are unjust, unreasonable, discriminatory, and in violation of 47 C.F.R. § 51.321 (id.).[5]

GNAPs argues that Verizon failed to demonstrate how its new procedures relate to any existing security concerns (id. at 7; GNAPs Reply Brief at 1). GNAPs argues that Verizon admits that it has never suffered a security breach that involved an individual who was either under the influence of drugs or who had a felony conviction (GN-VZ 1-3; GN-VZ 1-8; GNAPs Brief at 7-8). Moreover, GNAPs argues that Verizon does not use CLEC employees' social security numbers, or dates and places of birth, for any legitimate security purpose (GNAPs Brief at 8; GNAPs Reply Brief at 2). GNAPs argues that despite Verizon's insistence that it could not accomplish its security goals without such personal information about CLEC employees, GNAPs argues that Verizon could implement an alternative system which does not require the use of personal information, such as those used by the Massachusetts Registry of Motor Vehicles and the Federal Aviation Administration (GN-VZ 1-13; GNAPs Brief at 9;

---

[5] Pursuant to 47 C.F.R. § 51.321, "[A]n incumbent LEC shall provide, on terms and conditions that are just, reasonable, and non-discriminatory in accordance with the requirements of this part, any technically feasible method of obtaining interconnection or access to unbundled network elements at a particular point upon request by a telecommunications carrier."

GNAPs Reply Brief at 2). In addition, GNAPs states that by using card key systems, video monitors and the like, Verizon can increase its security without unduly intruding into the privacy of CLEC employees (GNAPs Brief at 9; GNAPs Reply Brief at 2). GNAPs also argues that Verizon admits that its new requirements apply in a discriminatory manner only to new applicants and to CLEC employees with expired badges, and not to CLEC employees who submit renewal applications prior to the expiration of their badges (GNAPs Reply Brief at 2). According to GNAPs, Verizon has not articulated why new CLEC employees and CLEC employees with expired badges pose more of a security threat than those CLEC employees hired before the new procedures went into effect or CLEC employees who renew their badges before expiration (id. at 2).

GNAPs also contends that requiring CLECs to provide certification of employee drug tests and background checks in order to access Verizon's COs constitutes a barrier to entry because CLECs would be required to spend additional time, money, and resources to develop, implement, and administer the drug testing programs and procedures for conducting criminal background checks (DTE-GN 1-1; VZ-GN 1-5; GNAPs Brief at 9; GNAPs Reply Brief at 1). Moreover, while GNAPs shares the Department's and Verizon's security concerns, GNAPs states that it also recognizes and respects the rights of its employees to protect their personal information (GNAPs Brief at 10). GNAPs argues that, given that identity theft is on the rise world-wide, the Department should weigh Verizon's interests in using a social security number-based system (that Verizon has designed for its own convenience) with the legitimate privacy interests of CLEC employees (DTE-GN 1-6; GNAPs Brief at 10).

Further, GNAPs argues that Verizon's drug testing requirement violates the Massachusetts Civil Rights Act and the right to privacy under G.L. c. 214, §1B, because Verizon has no reason to believe that CLEC employees are impaired by drugs or that the health and safety of CLEC and Verizon employees, or the safety of their equipment, are in jeopardy or at immediate risk (GNAPs Brief at 10-11). In addition, GNAPs states that 47 C.F.R. § 51.323(h)(2)(i) specifically addresses and identifies the reasonable security measures that an ILEC may adopt,[6] and because those measures do not include drug testing, criminal background checks, or any other measures that are invasive to an employee's privacy interest, GNAPs argues that the FCC's intention was to focus on infrastructure security

---

[6] In 47 C.F.R. § 51.323(h)(2)(i), the FCC identified the following collocation security measures as reasonable steps that an ILEC may undertake:

> (1) Installing security cameras or other monitoring systems; or
> (2) Requiring [C]LEC personnel to use badges with computerized tracking systems; or
> (3) Requiring [C]LEC employees to undergo the same level of security training, or its equivalent, that the incumbent's own employees, or third party contractors providing similar functions, must undergo provided, however, that the [I]LEC may not require [C]LEC employees to receive such training from the [I]LEC itself, but must provide information to the [C]LEC on the specific type of training required so the [C]LEC's employees can conduct their own training.
> (4) Restricting physical collocation to space separated from space housing the [I]LEC's equipment [if specific conditions are met].
> (5) Requiring the employees and contractors of collocating carriers to use a central or separate entrance to the incumbent's building, provided, however, that . . . employees and contractors of the [I]LEC's affiliates and subsidiaries must be subject to the same restriction.
> (6) Constructing or requiring the construction of a separate entrance to access physical collocation space, provided that [specific conditions are met].

measures and employee training only (id. at 11-12). GNAPs argues that the lack of any existing security problems with CLEC employees, the fact that CLEC employees operate solely CLEC-owned equipment, and the existence of on-site security measures at Verizon's premises, all erode Verizon's purported justification for its new and intrusive requirements for access card issuance (id. at 11).

Moreover, GNAPs argues that Verizon has failed to demonstrate how its new requirements directly address the threat posed by increased terrorist activity, and argues that Verizon cannot force CLECs to violate the constitutional and statutory rights of their employees under the guise of unidentified security concerns (VZ-GN 1-14; GNAPs Brief at 11). GNAPs urges the Department to deny Verizon the ability to require CLECs to implement drug testing or criminal background checks, or to require CLEC employees to provide their social security numbers and dates and places of birth (GNAPs Brief at 12). In the event the Department approves Verizon's new requirements, GNAPs requests that the Department order Verizon to bear the costs of CLECs' administration and implementation of any new procedures because Verizon unilaterally decided to change its requirements and invade the privacy of CLEC employees (id.).

B. Verizon

Verizon states that GNAPs' complaint is "frivolous and irresponsible," and that GNAPs is seeking to evade any responsibility to protect the security of critical telecommunications network facilities, or to preserve the safety of GNAPs' and Verizon's employees (VZ Brief at 1). Verizon asserts that GNAPs has no security standards, no formal employee screening procedures, and conducts no criminal background checks or drug tests of

its own employees or vendors (id. at 2). This, according to Verizon, underscores the reasonableness of, and need for, Verizon's security measures (id. at 2; VZ Reply Brief at 2, 4). Verizon states that, although the Department has been investigating Verizon's overall collocation security measures in a companion proceeding, D.T.E. 02-8,[7] GNAPs is the only CLEC that has challenged Verizon's new collocation access card and identification badge application requirements (VZ Brief at 1 n.1). In fact, argues Verizon, other CLECs testified in the D.T.E. 02-8 proceeding that they have implemented procedures similar to Verizon's for their own employees (id.).

Verizon asserts that the FCC's Advanced Services Order[8] permits reasonable collocation security arrangements that must apply equally to ILEC and CLEC employees (id. at 3). Verizon argues that, contrary to GNAPs' position, the Advanced Services Order identifies examples of the types of security devices that ILECs may utilize to protect and secure their facilities, but that these examples are intended as guidelines and not as an all-inclusive list (VZ Reply Brief at 5).

Moreover, Verizon argues that its new requirements regarding criminal background checks and drug tests apply not only to all collocators, but also to Verizon's own employees (VZ Brief at 4; VZ Reply Brief at 1, 6). Verizon argues that its new requirements do not

---

[7] 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, D.T.E. 02-8, Vote and Order To Open Investigation (January 24, 2002) ("Collocation Security Proceeding").

[8] Deployment of Wireline Services Offering Advanced Telecommunications Capability, CC Docket No. 98-147, First Report and Order and Further Notice of Proposed Rulemaking, FCC 99-48, (rel. March 31, 1999) ("Advanced Services Order").

contravene the letter or intent of the FCC's rules governing the provision of collocation or the prohibition against barriers to entry under the Telecommunications Act of 1996[9] (VZ Brief at 5). Moreover, Verizon argues that GNAPs' position that a requirement for CLECs to certify drug testing of their employees would unduly infringe on the employees' privacy rights is without merit (VZ Brief at 6). Verizon asserts that the Massachusetts courts apply a balancing test with respect to employees' privacy rights, and Verizon argues that the legitimate interest in the security of its COs, and the safety-sensitive nature of the employees' occupation (which requires heightened alertness and care) outweigh any perceived privacy concerns (id. at 6).

Similarly, Verizon argues that its new requirement that CLECs perform criminal background checks on their employees seeking access to Verizon's COs complies with applicable restrictions under Massachusetts law because Verizon requests certification concerning felony convictions only (GN-VZ 1-1; VZ Brief at 7-8). Moreover, Verizon argues that this requirement constitutes a reasonable security measure that is permissible under FCC rules (VZ Brief at 8).[10] Therefore, argues Verizon, GNAPs' effort to avoid this requirement is completely unwarranted and should be rejected by the Department (id.).

In addition, Verizon argues that requiring CLECs to provide social security numbers, and other personal information regarding CLEC employees on access card

---

9 Pub. L. No. 104-104, 110 Stat. 56 (1996), codified at 47 U.S.C. §§ 151 et seq. ("Telecommunications Act").

10 Verizon indicates that it would not necessarily deny issuance of an access card for an applicant with a felony conviction (see GN-VZ 1-1). Rather, Verizon would consider several factors consistent with its own internal hiring criteria, such as: 1) the severity of the offense; 2) the time elapsed since the completion of the sentence; 3) evidence of rehabilitation (e.g., successfully held other jobs); and 4) job relevance (i.e., the relationship of the offense to the position for which the individual has applied) (id.).

applications, does not unduly infringe on CLEC employees' rights under state or federal law (id.). Verizon argues that the federal privacy statutes GNAPs relies upon in its Complaint (i.e., 5 U.S.C. §§ 552 et seq.) (see GNAPs Complaint at ¶ 15) apply only to records held by the federal government and does not prevent employers from requesting employees' social security numbers (VZ Brief at 8-9). Verizon argues that it requests the same information from CLEC employees as it does from its own employees, which is in accordance with the FCC's "most stringent" rules for security arrangements[11] (GN-VZ 1-12; VZ Brief at 9). In addition, Verizon argues that, contrary to GNAPs' claims, the Massachusetts Registry of Motor Vehicles does require an individual's social security number on new driver's license applications and license renewals (VZ Reply Brief at 3). Verizon argues that it uses CLEC employee social security numbers, and dates and places of birth, to verify definitively an individual's identity before issuing or renewing a non-employee access card and identification badge (id. at 2). Verizon argues that it securely maintains this information in a password protected database with no outside access or system links, and access to the information is restricted to personnel in Verizon's Collocation Care Center and Corporate Security Department (DTE-VZ 1-1; VZ Brief at 9; VZ Reply Brief at 3).

---

[11] See Advanced Services Order at ¶ 47:

> [I]ncumbent LECs may impose security arrangements that are as stringent as the security arrangements that incumbent LECs maintain at their own premises either for their own employees or for authorized contractors. To the extent existing security arrangements are more stringent for one group than for the other, the incumbent may impose the more stringent requirements.

Verizon argues that GNAPs' hiring practices are unacceptable from a security perspective and should not be the standard used for determining reasonable security measures in Verizon's collocated COs (VZ Brief at 10). Verizon argues that there is no legal basis or "privacy principle" that warrants the elimination of Verizon's drug testing and criminal background check requirements, nor is there a regulatory imperative that would justify less stringent security measures for CLEC employees than Verizon applies to its own employees (id. at 11). In addition, Verizon states that GNAPs fails to demonstrate how compliance with Verizon's new security requirements would be costly or create a barrier to entry (id.). Verizon argues that the fact that GNAPs does not currently have any employee screening procedures of its own is no excuse for GNAPs' non-compliance with Verizon's requirements (id.). Verizon requests that the Department direct GNAPs to comply fully with Verizon's security procedures for the issuance of non-employee access credentials, so that Verizon can better protect its network and employees, as well as CLEC equipment and employees, in a time of heightened security concerns (id. at 13; VZ Reply Brief at 6-7).

III. ANALYSIS AND FINDINGS

A. Introduction

We begin our analysis with a brief discussion of the relationship between the Department's ongoing Collocation Security Proceeding (i.e., D.T.E. 02-8) and this proceeding.[12] In D.T.E. 02-8, we are investigating Verizon's overall collocation security policies in a proceeding that was initiated "in light of the heightened security concerns after the

---

[12] Without prejudging the issue in D.T.E. 02-8, we take administrative notice of the record in that matter noting that it has already been brought into play in the instant docket (see VZ Brief at 1 n.1).

events of September 11, 2001." D.T.E. 02-8, at 1 (January 24, 2002). That investigation has a much broader scope than the instant proceeding. In D.T.E. 02-8, the Department is examining the following issues:

> (1) the extent and nature of appropriate access by personnel of other carriers to Verizon central offices and other facilities for accessing collocation sites; (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 6. Conversely, in the instant case we are evaluating the discrete, single issue raised by GNAPs' Complaint; that is, whether Verizon's revised requirements for issuance of collocation access cards and identification badges are reasonable and in accordance with state and Federal law.[13]

In the past, both the FCC and the Department have addressed collocation issues. In various proceedings, the Department has implemented the FCC's determinations that the Telecommunications Act not only requires ILECs to allow CLECs to collocate equipment at ILEC COs, but also allows ILECs to require reasonable security arrangements to protect ILEC equipment and ensure network reliability, without unreasonably restricting CLECs' access to

---

[13] In D.T.E. 02-8, Verizon indicated in its Initial Testimony that it "plans to implement an in-depth, pre-screening of collocated carrier personnel designated to access physical collocation arrangements in its COs as a requirement of providing identification badges. This is consistent with Verizon's more stringent pre-screening and background checks for its employees and vendors that are being adopted as part of its nationwide efforts to enhance security in its COs since September 11th" (see Exh. VZ-1, at 5 (D.T.E. 02-8)). Although Verizon indicated in D.T.E. 02-8 that it had plans to implement revised collocation access card and identification badge requirements, Verizon did not introduce the specifics of its post-August 2002 requirements as part of its proposal in D.T.E. 02-8.

their collocated equipment. See, generally, Teleport Petition, D.T.E. 98-58 (1999); Verizon Tariff M.D.T.E. No. 17, D.T.E. 98-57 (March 24, 2000); Verizon Tariff M.D.T.E. No. 17, D.T.E. 98-57-Phase I (September 7, 2000). The FCC specifically addressed collocation security issues in its Advanced Services Order at ¶¶ 46-49,[14] and has determined that the use of badges for non-employees is one of a number of reasonable collocation security measures that an ILEC may undertake. See Advanced Services Order at ¶ 48 (see also n.6, above). However, the FCC has not addressed what type of information an ILEC may require from CLEC employees as a condition of badge issuance, save for what may fairly be inferred from 47 C.F.R. § 51.323(h)(2)(i) and from the central fact that the ILEC is ultimately responsible for overall system security through measures even-handedly applied.[15]

B. Personal Information on Card Applications

For the following reasons, we do not agree with GNAPs that Verizon's requirement that CLEC employees who access Verizon's COs must provide Verizon with personal information, such as social security numbers, and dates and places of birth, is "irrelevant to Verizon, an intrusion into the privacy of [GNAPs] employees and achieves no legitimate security interest" (see GNAPs Brief at 4). We determine that Verizon has provided a

---

[14] On March 17, 2000, the U.S. Court of Appeals for the District of Columbia Circuit ("D.C. Circuit") affirmed in part, and vacated in part, the FCC's Advanced Services Order. See GTE Service Corp. v. Federal Communications Comm'n, 205 F.3d 416 (D.C. Cir. 2000). The D.C. Circuit remanded to the FCC paragraph 42 of the Advanced Services Order which broadly defined the terms "necessary" and "physical collocation." Id. at 427. The D.C. Circuit denied review of the remaining portions of the Advanced Services Order, including the collocation security provisions. See id.

[15] See also n.16, below.

reasonable basis for requesting this information, and that, in doing so, Verizon's actions do not compromise CLEC employees' privacy interests.

Verizon has stated that it uses the information supplied on a CLEC employee's card application to compare against Verizon's internal records for previous employment with Verizon and cause of termination occurrences or for any previous instances of misconduct as a CLEC employee while on Verizon's premises (GN-VZ 1-10; GN-VZ 1-14). Verizon has also indicated that it uses this information to permit non-employee access to COs in the event of a malfunctioning CO access system by requesting oral confirmation of this information from the assigned cardholder (DTE-VZ 1-2). The Department recognizes that Verizon must have certain information key to security that is unique to each individual working on or near sensitive equipment which is readily known only by such workers (such as social security numbers, or dates and places of birth). Without routinely requiring such information, Verizon may not verify with certainty the identity of a non-employee cardholder before allowing authorized entry into Verizon's COs. Further, requesting information that enables Verizon to confirm prior employment with Verizon or prior occurrences of misconduct is a legitimate use of this information in order to protect the safety of Verizon's equipment and employees. Moreover, existing provisions in M.D.T.E. Tariff No. 17 give Verizon the authority to require specific forms of identification from CLEC employees who access Verizon's COs.[16]

---

[16] See M.D.T.E. Tariff No. 17, Part E, 2.2.5 Safety and Security Measures:

> D. The CLEC will supply the Telephone Company with a list of employees or approved vendors who require access. The list will include social security numbers of all such individuals or an alternative form of identification as specified by the

(continued...)

Therefore, we determine that Verizon has provided a reasonable basis for requiring personal information from CLEC employees, such as social security numbers and dates and places of birth, on its collocation access card and identification badge applications.

Moreover, the Department determines that Verizon's requirement to provide this information does not compromise the privacy of CLEC employees because Verizon utilizes measures to safeguard this information properly.[17] However, in order for Verizon's requirement that CLECs provide this personal information to remain reasonable, we determine that Verizon must continue to employ special measures to protect this information from disclosure, and must not use this information for any purpose unrelated to security. See D.T.E. 03-29, at 3-4, Hearing Officer Ruling on Global NAPs, Inc.'s Motion for Confidential Treatment (May 27, 2003) (extending confidential protection to information request response containing GNAPs employees' social security numbers).

---

[16](...continued)

Telephone Company. All individuals must be U.S. citizens where required by law or regulation.

[17] Verizon states that information obtained from collocation access card and identification badge applications is securely maintained at Verizon's Collocation Care Center and Corporate Security Department, and that only those personnel who are responsible for processing the applications or issuing cards have access to the secured databases and files where this information is stored (see DTE-VZ 1-1).

C. Drug Tests and Criminal Background Checks

We next turn to Verizon's requirements pertaining to CLEC employee drug tests and criminal background checks.[18] For the reasons discussed below, we determine that Verizon's provision on its card applications that CLECs certify that their employees who seek access to Verizon's COs have undergone a drug test and background check for felony convictions is a reasonable security measure that Verizon may adopt to safeguard its equipment and ensure network reliability.

We do not agree with GNAPs that the FCC's intention in promulgating its regulations concerning collocation security "was to focus on infrastructure security measures and employee training" only (GNAPs Brief at 12) or GNAPs' position that "[i]f drug/alcohol screening or criminal background investigations were intended, then Congress would have included these measures" (id.). Rather, we determine that the "reasonable security measures" identified by the FCC in 47 C.F.R. § 51.323(h)(2)(i), and subsections (1)-(3), are not intended as an exhaustive list of ILECs' security options, and that other options can also be considered

---

[18] According to Verizon's "Instructions for Completing and Submitting Verizon Collocation Access Card and Identification Badge Application Forms," an authorized representative of the CLEC must certify that a background investigation and drug test were conducted for the applicant and that the applicant has:

> a. No felony convictions for the seven years prior to the date of the background investigation, and that the Collocator or its contractor has no knowledge of any felony convictions after the date of the background investigation.
> b. Had a drug screening performed as part of the background investigation . . . and that there was no indication of the presence of marijuana, cocaine, opiates, phencyclidine or amphetamines in the body.

(VZ Answer, Att. 1).

reasonable security measures under the FCC's directives. Section 51.323(h)(2)(i) must be read in conjunction with the FCC's Advanced Services Order at ¶ 48, which states, "We permit incumbent LECs to install, for example, security cameras or other monitoring systems, or to require competitive LEC personnel to use badges with computerized tracking systems" (emphasis added). The use of the phrase "for example" clearly indicates that the FCC did not intend these measures to be an exhaustive list, but rather to serve as examples of reasonable security measures that an ILEC may adopt. Therefore, we do not deny Verizon the ability to require certification of drug tests or criminal background checks, as GNAPs has requested, merely because those measures were not specifically identified by the FCC in 47 C.F.R. § 51.323(h)(2)(i).

Moreover, Verizon does not require of collocated CLECs anything in this regard that Verizon does not impose on its own employees and contractors. As part of its own internal personnel security standards, Verizon requires its new employees to undergo drug tests and criminal background checks prior to an offer of employment and receipt of CO access credentials (see GN-VZ 1-1). Although Verizon does not have the authority to require CLECs to adopt this employee pre-screening process as part of their general hiring practices, Verizon does have the authority under FCC requirements to impose its own CO security procedures on CLEC employees prior to granting non-employees access to its COs.[19] While we agree that it is important to be able to identify readily when an unauthorized person has gained access to Verizon's COs (through the use of security cameras or guards, for instance), it is equally

---

[19] Pursuant to 47 C.F.R. § 51.323(h)(2)(i), "An incumbent LEC may only impose security arrangements that are as stringent as the security arrangements that the incumbent LEC maintains at its own premises for its own employees or authorized contractors."

important to insist that a CLEC conduct pre-screening of potential access cardholders to determine if a particular individual poses an increased risk to the facilities, equipment, and personnel of both Verizon and CLECs prior to receiving entry authorization in the form of identification badges and access cards.[20] Because Verizon applies these requirements equally to its own employees and contractors who have access to Verizon's COs as it does to CLEC employees who have access to Verizon's COs, the Department determines that drug tests and criminal background checks comply with both the FCC's regulations and the Department's own requirements, and constitute a reasonable means to protect Verizon's network and facilities.[21]

GNAPs raises an important issue, however, with respect to the application of Verizon's requirements on those CLEC employees seeking renewal of an already expired collocation access card and identification badge. The FCC has stated that "[t]o be nondiscriminatory, a practice must apply equally, both on its face and in actual execution, to the incumbent's own technicians and contractors and to each collocator's technicians and contractors."[22] Verizon requires CLEC employees whose badges have expired, no matter how

---

20 See D.T.E. 02-8, at 6 (January 24, 2002) (emphasizing the importance of preventive, rather than after-the fact, collocation security measures).

21 We clarify that, if a CLEC employee indicates on his access card application that he has had a felony conviction in the seven years prior to, or after the date of, the background investigation, Verizon must provide the CLEC employee with the opportunity to provide additional information in support of his application, consistent with Verizon's own internal hiring criteria. See n.10, above.

22 In the Matters of Deployment of Wireline Services Offering Advanced Telecommunications Capability, CC Docket 98-147, Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, CC Docket No 96-98,

(continued...)

long or short a time the badge has been expired, to undergo a background investigation and drug test prior to card renewal, yet Verizon exempts its own former employees who are rehired within one year of the separation date (i.e., the last date their Verizon employee access cards and identification badges would have been effective) from undergoing a background investigation (see GN-VZ 1-1, Att. A at 1). In order for these procedures to be nondiscriminatory, the Department instructs Verizon to extend for a period of one year from the expiration date of a CLEC employee's access card and identification badge an exemption from the background investigation requirement contained on Verizon's application for collocation access cards and identification badges.[23] In short, whatever vetting Verizon requires of CLEC employees for access to critical facilities and the equipment housed there should be required of Verizon's employees too.

We also do not agree with GNAPs that Verizon's drug test requirement violates Massachusetts privacy law. The right to privacy under G.L. c. 214, § 1B, is not absolute.[24] In an employment setting, such as here, an individual's privacy interest must be balanced against the interest in determining that individual's effectiveness in his or her job, as well as the interest in ensuring public safety. See Webster v. Motorola, 418 Mass. 425, 431-32 (1994);

---

[22](...continued)
Order on Reconsideration and Second Further Notice of Proposed Rulemaking in CC Docket No. 98-147 and Fifth Further Notice of Rulemaking in CC Docket No. 96-98, FCC 00-297, at ¶ 60 (rel. August 10, 2000) (discussing "safe-time" work practices).

[23] As noted above, CLEC employees who renew their badges prior to the expiration date are also exempt from the background investigation requirement.

[24] G.L. c. 214, §1B states, "A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages."

Folsmbee v. Tech Tool Grinding & Supply, Inc., 417 Mass. 388, 392 (1994); Bratt v. International Business Machines, Corp., 392 Mass. 508, 524 (1984). The Department recognizes the role that telecommunications infrastructure plays in contributing to public safety, and the importance of protecting and maintaining the security of the network. See D.T.E. 02-8, at 6 (January 24, 2002) ("[In opening our investigation into collocation security, o]ur intent is to ensure that reliable service to competing telecommunications service providers, businesses, and residents of the Commonwealth is not unreasonably at risk"). And we agree with Verizon that it has a legitimate business interest in ensuring the reliability of the telecommunications network, as well as the safety of its own employees (see VZ Brief at 6). Moreover, we have determined above that Verizon's drug test certification requirement for CLEC employees who seek access to Verizon's COs is a reasonable security measure consistent with FCC rules. Therefore, we conclude that G.L. c. 214, § 1B, does not preclude Verizon from requiring certification of CLEC employee drug tests on its collocation access card and identification badge application.

Next we turn to GNAPs' assertion that requiring CLEC access card and identification badge applicants to undergo drug tests and criminal background checks constitutes a barrier to entry.[25] We do not agree. GNAPs argues that "[r]equiring Global and other CLECs to undergo burdensome and intrusive procedures under the guise of security will

---

[25] The Department has previously stated that a barrier to entry is any factor that prevents firms from operating in a particular market. Barriers to entry are divided into four general categories: absolute cost advantage, economies of scale, product differentiation, and regulatory barriers. Verizon Alternative Regulation, D.T.E. 01-31-Phase I, at 43 (2002) (citing Edgar K. Browning and Mark A. Zupan, Microeconomic Theory and Applications 330 (5th ed. 1996)).

have an anti-competitive effect on CLECs in Massachusetts" (GNAPs Complaint at ¶ 12), and further explains that "CLECs will have to devote time and resources to implementing procedures [in compliance with Verizon's requirements]" (VZ-GN 1-5). However, GNAPs admits that it has not evaluated the costs required to implement Verizon's requirements (see VZ-GN 1-12), and GNAPs concedes that it "does not claim that the practices themselves are prohibitively expensive such that [GNAPs] could not compete were it required to institute these procedures" (VZ-GN 1-15). Rather, GNAPs argues that because Verizon's procedures violate state and Federal law, are intrusive, and do not accomplish any legitimate security interest, the mere imposition of the requirements is a barrier to entry (see id.). We determine that these reasons do not support GNAPs' argument that Verizon's requirements are a barrier to entry, but are more related to GNAPs' prior arguments, which we have already addressed, concerning whether Verizon's application requirements are reasonable and nondiscriminatory.[26] Therefore, we determine that Verizon's requirement that CLECs certify that drug tests and background checks have been performed on their employees entering Verizon's collocated COs does not constitute a barrier to entry for CLECs in Massachusetts.

Lastly, we address GNAPs' request that the Department order Verizon to bear the costs of GNAPs' implementation and administration of procedures in order for GNAPs to comply with Verizon's drug test and background check requirements (see GNAPs Brief at 12). We do not agree. In the Advanced Services Order at ¶ 48, the FCC instructs state

---

[26] We also note that some parties to the Department's D.T.E. 02-8 proceeding indicated that they have already implemented background check procedures for new employees similar to Verizon's requirements, which undermines GNAPs' claim that Verizon's requirements create a barrier to entry for CLECs (see VZ Brief at 1 n.1; see also Exh. Qwest-1, at 20; Exh. WCom-1, at 13 (D.T.E. 02-8)).

commissions to "permit incumbent LECs to recover the costs of implementing . . . security measures from collocating carriers in a reasonable manner." In addition, 47 C.F.R. § 51.323(h)(2)(i) states that "[a]n incumbent LEC may require a collocating carrier to pay . . . for the least expensive, effective security option that is viable for the physical collocation space assigned." Consistent with FCC's directives, because we have determined that Verizon's requirement for drug tests and criminal background checks for CLEC employees who access Verizon's COs is a reasonable security measure and consistent with applicable law, we do not agree that Verizon is required to pay for all CLECs' compliance with this security measure; rather it is a cost that must be borne by the CLECs that seek access to Verizon's collocated COs.[27]

D. Conclusion

In sum, we determine in this Order that Verizon's revised requirements for issuance of collocation access cards and identification badges are reasonable and consistent with Federal and state law. In reaching this conclusion, we have diligently addressed the many and varied claims that GNAPs has asserted in this proceeding. In closing, we deem it appropriate to make a few general comments. The events of September 11, 2001, marked a watershed in domestic security. Vulnerability of both ILEC and collocated CLECs' utility infrastructure

---

[27] See D.T.E. 98-57, at 193 (March 24, 2000):

> As the Department stated in its Phase 4-G Order, each portion of the network must carry its own weight (i.e., collocators should pay their own share of security cost required for each central office). . . . The various security investments are incremental investments caused by the need for CLECs to place their equipment in [Verizon's] central office.

and the adverse consequences to the public convenience were and continue to be vividly demonstrated by the direct damage to Verizon's 130 West Street building next to the World Trade Center in Manhattan. In revising its CO access card and identification badge requirements, Verizon has taken lawful, appropriate, and commendable steps to improve its internal security procedures. If competing carriers choose to operate their own employee vetting on a less stringent basis, that is no reason for the Department to require Verizon to roll the dice on the public's interest in CO security.

IV. ORDER

Accordingly, after due notice and consideration, it is

ORDERED: That the parties shall comply with all directives contained herein.

By Order of the Department,

_____/s/_____
Paul B. Vasington, Chairman

_____/s/_____
James Connelly, Commissioner

_____/s/_____
W. Robert Keating, Commissioner

_____/s/_____
Eugene J. Sullivan, Jr., Commissioner

_____/s/_____
Deirdre K. Manning, Commissioner

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 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. (Sec. 5, Chapter 25, G.L. Ter. Ed., as most recently amended by Chapter 485 of the Acts of 1971).