

FCC MAIL SECTION

~~MAR 10 11 28 AM '99~~

Federal Communications Commission

FCC 99-11

DISPATCHED BY Before the  
Federal Communications Commission  
Washington, D.C. 20554

In the Matter of )

Communications Assistance for Law )  
Enforcement Act )

CC Docket No. 97-213

REPORT AND ORDER

Adopted: January 29, 1999

Released: March 15, 1999

By the Commission:

I. INTRODUCTION

1. On October 10, 1997, the Commission released a Notice of Proposed Rulemaking in the above-docketed proceeding focusing on the specific responsibilities imposed upon the Commission to implement certain sections of the Communications Assistance for Law Enforcement Act (CALEA or the Act).<sup>1</sup> Since that time, the Commission has addressed two very significant CALEA implementation issues by granting a blanket extension of the Act's October 25, 1998 compliance deadline for all telecommunications carriers until June 30, 2000,<sup>2</sup> and by initiating a section 107(b) Further Notice of Proposed Rulemaking to resolve the dispute regarding the industry's interim standard, J-STD-025.<sup>3</sup> In this Order, we now establish the systems security and integrity regulations that telecommunications carriers must follow to comply with section 105 of CALEA.<sup>4</sup>

2. In prescribing these rules, we have fully considered the comments filed in response to the NPRM. As explained below, we take this action pursuant to the authority granted to the Commission under section 105 of CALEA and section 229 of the Communications Act of 1934, as amended. Accordingly, we conclude that telecommunications carriers must ensure that "any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative

<sup>1</sup> Communications Assistance for Law Enforcement Act, *Notice of Proposed Rulemaking*, 13 FCC Rcd 3149 (1997) (NPRM).

<sup>2</sup> In the Matter of Petition for the Extension of the Compliance Date under Section 107 of the Communications Assistance for Law Enforcement Act, *Memorandum, Opinion and Order*, 13 FCC Rcd 17,990 (1998) (*Extension Order*).

<sup>3</sup> In the Matter of Communications Assistance for Law Enforcement Act, *Further Notice of Proposed Rulemaking*, CC Docket No. 97-213, FCC 98-282 (rel. Nov. 5, 1998).

<sup>4</sup> 47 U.S.C. § 1004.

intervention of an individual officer or employee of the carrier"<sup>5</sup> acting in accordance with the regulations adopted herein.<sup>6</sup>

## II. BACKGROUND

3. CALEA, enacted on October 25, 1994, was intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently in the face of rapid advances in telecommunications technology.<sup>7</sup> In enacting this statute, however, Congress recognized the need to protect privacy interests within the context of court-authorized electronic surveillance. Thus, in defining the terms and requirements of the Act, Congress sought to balance three important policies: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."<sup>8</sup>

4. Section 105: Systems Security and Integrity. Section 105 of CALEA specifically seeks to ensure the protection of telecommunications carriers' systems security and integrity by requiring that "[a] telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission."<sup>9</sup> As the plain language of the statute emphasizes, the Commission has the authority to prescribe rules that telecommunications carriers must follow to accomplish this task. Section 301 of CALEA, amending the Communications Act of 1934 to add section 229, specifically grants the Commission the general authority to "prescribe such rules as are necessary to implement the requirements of the Communications Assistance for Law Enforcement Act."<sup>10</sup> More specifically, as section 229(b) directs, "[t]he rules prescribed pursuant to subsection (a) shall include rules to implement section 105 of the Communications Assistance for Law Enforcement Act."<sup>11</sup>

5. With this goal in mind, the NPRM tentatively concluded that section 105 of CALEA imposes a duty on each telecommunications carrier to ensure that only lawful interceptions will occur on its premises, and that unlawful interceptions occurring on its premises will constitute a violation of that duty.<sup>12</sup> We also tentatively concluded that this duty required each telecommunications carrier to ensure

---

<sup>5</sup> 47 U.S.C. § 1004.

<sup>6</sup> 47 U.S.C. § 1004; 47 U.S.C. § 229.

<sup>7</sup> 140 Cong. Rec. H-10779 (daily ed. October 7, 1994) (statement of Rep. Hyde).

<sup>8</sup> H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 13 (1994).

<sup>9</sup> 47 U.S.C. § 1004.

<sup>10</sup> 47 U.S.C. § 229(a).

<sup>11</sup> 47 U.S.C. § 229(b).

<sup>12</sup> NPRM at ¶ 26.

that employees designated to implement and have access to these interceptions would only perform authorized interceptions, and that they would not reveal the existence, or the content, of these interceptions to anyone other than authorized law enforcement personnel, except as required by a court of competent jurisdiction or appropriate legislative or regulatory body.<sup>13</sup>

6. To reconcile the different use of language between section 105 of CALEA and section 229 of the Communications Act, we tentatively concluded that Congress intended rules prescribed to implement CALEA security requirements to apply to all telecommunications carriers as that term is defined by section 102(8) of that statute.<sup>14</sup> We further concluded that section 105 of CALEA and section 229(b) of the Communications Act should be read consistently, and that the rules promulgated pursuant to section 229 shall apply to all telecommunications carriers as defined by section 102(8) of CALEA.<sup>15</sup>

7. Section 229(b)(1): Appropriate Policies and Procedures for Employee Supervision. The NPRM proposed various rules to implement section 105 of CALEA. First, we tentatively concluded that appropriate legal authorization for the purposes of CALEA should encompass what is required by 18 U.S.C. § 2518.<sup>16</sup> We therefore proposed a rule to require carriers to state in their internal policies and procedures that their personnel must receive a court order or, under exigent circumstances, an order from a specially designated investigative or law enforcement officer, before assisting law enforcement officials in implementing electronic surveillance.<sup>17</sup> Additionally, we proposed to require carriers to incorporate into their policies and procedures the list of the exigent circumstances found at 18 U.S.C. § 2518(7).<sup>18</sup>

8. Furthermore, to establish carriers' security policies, we examined the express language of section 229(b)(1) and proposed that the term "appropriate authorization," as used therein, should be defined as the authorization that a carrier's employee needs from the carrier to engage in interception activity.<sup>19</sup> Our proposals included a requirement for carriers to designate specific employees, officers, or both to assist law enforcement officials in implementing lawful interceptions and to indicate in their

---

<sup>13</sup> *Id.* at ¶ 26.

<sup>14</sup> *Id.* at ¶ 38.

<sup>15</sup> *Id.* at ¶ 38.

<sup>16</sup> *Id.* at ¶ 29. For example, to obtain a court order authorizing the interception of a wire, or electronic communication, a law enforcement officer must submit a written application to a court of competent jurisdiction. The application must include information such as the identity of the officer making the application, a complete statement of facts supporting the application, a statement of whether other investigative procedures have been tried and failed or of why they appear reasonably unlikely to succeed or are too dangerous to attempt, and a statement of the period of time for which the interception is required. 18 U.S.C. § 2518(1).

<sup>17</sup> NPRM at ¶ 29.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* at ¶ 25.

policies and procedures that only designated employees may conduct these interceptions.<sup>20</sup> We further proposed that non-designated employees be permitted to assist with certain legal surveillance work, provided that they did so without specific knowledge of the underlying interception and as part of their routine work assignments.<sup>21</sup> Moreover, because we determined that notations that non-designated employees might make while unknowingly effectuating electronic surveillance would not suffice for the purposes of CALEA, we proposed that carriers' designated employees were required to create separate records of electronic surveillance information to effectively supervise the electronic surveillance work of such non-designated employees.<sup>22</sup>

9. As a general matter, we sought comment on the nature of the information, if any, that telecommunications carriers should be required to make available to law enforcement officials upon request.<sup>23</sup> Specifically, we requested comment on whether our rules should require telecommunications carriers to create and maintain an official list of all personnel designated by the carriers to conduct lawful interceptions.<sup>24</sup> We also sought comment on whether carriers should be required to designate a senior officer or employee to serve as the point of contact for law enforcement officials.<sup>25</sup> Finally, we requested comment on the information that should be included on this list, and whether it should contain each designated employee's name, personal identifying information such as their date and place of birth, social security number, official title, and telephone and pager numbers.<sup>26</sup>

10. Section 229(b)(2): Maintaining Secure and Accurate Records. With regard to record keeping, the NPRM proposed a rule to require that telecommunications carriers' internal policies and procedures include a requirement that each employee and/or officer who knowingly conducts an interception sign an affidavit containing the following information prior to each instance of participation in an interception: (1) the telephone number(s) or the circuit identification number(s) involved; (2) the name of each employee and officer who effected the interception and possessed information concerning its existence, and their respective positions; (3) the start date and time of the interception; (4) the stop date and time of the interception; (5) the type of interception (e.g., pen register, trap and trace, etc.); (6) a copy or description of the written authorization for the employee and officer to participate in interception activity; and (7) a statement that the employee or officer will not disclose information about the interception to any person not properly authorized by statute or court order.<sup>27</sup> We also sought comment on whether additional items should be included in each affidavit, and whether we should limit the number

---

<sup>20</sup> *Id.* at ¶ 30.

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> NPRM at ¶ 33.

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

<sup>27</sup> *Id.* at ¶ 31.

of affidavits by requiring that an affidavit be prepared only by the employee responsible for the interception activity.<sup>28</sup>

11. Under section 229(b)(2), we also proposed to require carriers to keep records of all interceptions, regardless of whether they were conducted with or without lawful authorization.<sup>29</sup> We proposed that each record include the following information: (1) the telephone number(s) and circuit identification number(s) involved; (2) the start date and time of the interception; (3) the stop date and time of the interception; (4) the identity of the law enforcement officer presenting the authorization; (5) the name of the judge or prosecuting attorney signing the authorization; (6) the type of interception (e.g., pen register, trap and trace, etc.); and (7) the name(s) of all telecommunications carrier personnel involved in performing, supervising, and internally authorizing, the interception and the names of those who possessed knowledge of the interception.<sup>30</sup> We further proposed that such records be compiled, either contemporaneously with each interception, or within 48 hours of the start of each interception.<sup>31</sup> We sought comment on the length of time each record should be retained within the custody of each telecommunications carrier,<sup>32</sup> and noted that 18 U.S.C. § 2518(8)(a) requires law enforcement to retain intercepted communications for, at a minimum, ten years.<sup>33</sup>

12. Sections 229(b)(3) and 229(c): Submission of Policies and Procedures and Commission Review. To establish procedures for the submission of carriers' policies and procedures to the Commission under section 229(b)(3), we sought comment regarding whether we should differentiate between small and large carriers in terms of those requirements.<sup>34</sup> We also sought comment on ways to implement CALEA that would be consistent with congressional intent and would also reduce CALEA compliance burdens on small carriers.<sup>35</sup> If the record indicated that it was in the public interest to minimize the burdens imposed on small incumbent local exchange carriers, we proposed defining "small telecommunications carriers" for incumbent local exchange carriers (ILECs) in terms of the indexed revenue threshold provided in 47 C.F.R. § 32.9000, so that telecommunications carriers may determine the indexed revenue threshold annually.<sup>36</sup> For carriers with annual revenues from telecommunications operations exceeding that threshold, we proposed, pursuant to section 229(c)(3), to require individual filings with the Commission

---

<sup>28</sup> *Id.*

<sup>29</sup> NPRM at ¶ 32.

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> *Id.* at ¶ 34.

<sup>35</sup> NPRM at ¶ 35.

<sup>36</sup> *Id.*

that contain detailed statements of the policies, processes, and procedures that each carrier would use to comply with the requirements that are imposed by CALEA and by Commission rules.<sup>37</sup>

13. We further proposed to permit any ILEC with annual operating revenues from telecommunications services of less than the threshold to elect to either: (1) file a statement describing its security policies, processes, and procedures; or (2) certify that it observes procedures consistent with our prescribed systems security rules.<sup>38</sup> We stated that those ILECs that do not choose to certify compliance with CALEA's requirements must submit their policies and procedures to the Commission for individual review.<sup>39</sup> We sought comment for alternative proposals.<sup>40</sup> Additionally, we requested comment regarding whether we should use such a demarcation point for other classifications of telecommunications common carriers such as cable operators, competitive access providers, or CMRS providers.<sup>41</sup> We also sought comment on whether we should adopt the same threshold or a lower dollar threshold for streamlined filing requirements for other telecommunications carriers with CALEA obligations.<sup>42</sup>

14. Pursuant to 229(c), we requested comment on the date by which carriers should be required to file their initial procedures and certifications with the Commission.<sup>43</sup> We tentatively concluded that 90 days from the effective date of the rules adopted in this proceeding should be sufficient time for carriers to complete and file their policies and procedures with the Commission.<sup>44</sup> We recognized that as technological advances occur, companies will merge or divest creating a continuing need for carriers to update policies and procedures. Thus, we also requested comment on the time that carriers should have, preceding and following a merger or divestiture, to make a new filing.<sup>45</sup>

15. Section 229(d): Penalties. Finally, we sought comment on whether the procedures and penalties for violations of Commission rules by common carriers in sections 503(b) of the Communications Act and 1.8 of the Commission's rules should be applied to all entities that are subject to CALEA.<sup>46</sup> We also requested comment on the extent to which a telecommunications carrier's duty to conduct only lawfully authorized interceptions extends vicarious criminal and civil liability to a carrier if

---

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> *Id.*

<sup>41</sup> NPRM at ¶ 36.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.* at ¶ 37.

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

the carrier's employees are convicted of conducting illegal electronic interceptions.<sup>47</sup> We further requested comment on whether a Commission rule that requires carriers to report all illegal wiretapping and compromises of the confidentiality of the interception, to the Commission and/or the affected law enforcement agency or agencies, would modify or mitigate the carrier's liability under 18 U.S.C. §§ 2511 and 2520.<sup>48</sup>

### III. DISCUSSION

#### A. The Commission's Authority to Prescribe "Necessary" Rules

16. As explained above, sections 229(a) and (b) of the Communications Act authorize the Commission to "prescribe such rules *as are necessary* to implement the requirements of the Communications Assistance for Law Enforcement Act,"<sup>49</sup> including the rules to implement section 105 of that Act.<sup>50</sup> In response to the NPRM, several commenters expressed concern that the Commission's proposed regulations to implement section 105 of CALEA were unduly burdensome.<sup>51</sup> Some commenters argue that section 105 regulations are not "necessary" under the language of section 229(a) because carriers already have sufficient policies and procedures in place.<sup>52</sup> For instance, the United States Telephone Association (USTA) maintains that the record does not support the necessity of creating section 105 rules.<sup>53</sup> Likewise, BellSouth contends that the Commission's proposals for additional rules are unwarranted because its current practices suffice to comply with section 105.<sup>54</sup> BAM suggests that the Commission is directed under CALEA to take a measured approach to imposing new regulations and that "[n]ew rules should . . . not be imposed unless they are shown to be clearly necessary."<sup>55</sup> Law

---

<sup>47</sup> NPRM at ¶ 27.

<sup>48</sup> *Id.*

<sup>49</sup> 47 U.S.C. § 229(a) (emphasis added).

<sup>50</sup> 47 U.S.C. § 229(b).

<sup>51</sup> GTE Service Corporation (GTE) Comments at 7; Omnipoint Communications, Inc. (Omnipoint) Comments at 4; Bell Atlantic Mobile (BAM) Comments at 4; Sprint Spectrum L.P. (Sprint Spectrum) Comments at 1; Powertel, Inc. (Powertel) Comments at 3; AT&T Corporation and AT&T Wireless Services, Inc. (AT&T) Comments at 28; Omnipoint Reply Comments at 2; AT&T Reply Comments at 20; Motorola, Inc. (Motorola) Reply Comments at 9; AirTouch Communications, Inc. (AirTouch) Reply Comments at 16-17; PrimeCo Personal Communications, Inc. (PrimeCo) Reply Comments at 7; Cellular Telecommunications Industry Association (CTIA) Reply Comments at 19; Nextel Communications, Inc. (Nextel) Reply Comments at 9.

<sup>52</sup> GTE Comments at 7; BAM Comments at 3-4; SBC Communications (SBC) Comments at 17; Sprint Spectrum Comments at 1; U S West, Inc. (U S West) Reply Comments at 7; GTE Reply Comments at 7; SBC Reply Comments at 4; Telecommunications Industry Association (TIA) Reply Comments at 13.

<sup>53</sup> United States Telephone Association (USTA) Comments at 5.

<sup>54</sup> BellSouth Corporation, BellSouth Telecommunications, Inc., BellSouth Cellular Corporation, BellSouth Personal Communications, Inc. and BellSouth Wireless Data, L.P. (BellSouth) Comments at 8.

<sup>55</sup> BAM Comments at 4.

enforcement, on the other hand, emphasizes the need for system security and integrity regulations to ensure that internal carrier authorizations and procedures are designed to maintain the timeliness, security, and accuracy of intercepts.<sup>56</sup>

17. Decision. Based upon the record before us, we find that, pursuant to our statutory authority, it is necessary for us to implement a very limited set of rules to assist telecommunications carriers in complying with their obligations under section 105 of CALEA and sections 229(b) and (c) of the Communications Act. The plain language of section 105 of CALEA and sections 229(b) and (c) of the Communications Act reflects a congressional concern regarding the necessity of rules to ensure that carriers have policies and procedures in place that require the affirmative intervention and knowledge of their employees of any interception being effected through their switching premises, and that such interception is done lawfully and carefully documented. Further, the legislative history of CALEA indicates that section 105 of the Act was enacted to "make clear that government agencies do not have the authority to activate remotely interceptions within the switching premises of a telecommunications carrier. Nor may law enforcement enter onto a telecommunications carrier's switching office premises to effect an interception without the carrier's prior knowledge and consent when executing a wiretap under exigent or emergency circumstances . . . All executions of court orders or authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier."<sup>57</sup>

18. While the Commission acknowledges that certain carriers currently have existing policies and procedures in place to secure and protect their telecommunications systems in a manner that would comply with section 105 of CALEA and sections 229(b) and (c) of the Communications Act, we find that more recent entrants to the market are not as well equipped or prepared. For example, in the context of arguing that administrative costs will attach to the implementation of section 105 regulations, Nextel explains that "[w]hile cellular providers and incumbent LECs may have established wiretap compliance teams and processes, new entrants such as Nextel, PCS carriers and competitive LECs, have not had the opportunity to establish internal processes."<sup>58</sup> We conclude that it is precisely this void that the rules adopted herein are directed to fill. Accordingly, we find that it is necessary to implement a minimum set of requirements that all telecommunications carriers must follow to ensure compliance with section 105 of CALEA and sections 229(b) and (c) of the Communications Act. In so doing, however, we decline to adopt specific or detailed policies and procedures that telecommunications carriers must include within their internal operating practices pursuant to section 105 of CALEA or sections 229(b) or (c) of the Communications Act because we agree that it is not the Commission's responsibility to "micro-manage" telecommunications carriers' corporate policies.<sup>59</sup> Rather, the rules we adopt herein serve to provide telecommunications carriers with guidance for the minimum requirements necessary to achieve compliance with section 105 of CALEA and sections 229(b) and (c) of the Communications Act in the least burdensome manner possible.

---

<sup>56</sup> United States Department of Justice and Federal Bureau of Investigation Joint Comments (FBI Comments) at 24.

<sup>57</sup> H. Rep. No. 103-837 at 23, reprinted in 1994 U.S.C.C.A.N. 3489.

<sup>58</sup> Nextel Comments at 14; *see also* Nextel Reply Comments at 9.

<sup>59</sup> *See* BAM Comments at 3.

**B. Section 229(b): Rules to Implement Section 105**

19. Section 229(b) specifically directs that "[t]he rules prescribed pursuant to subsection (a) shall include the rules to implement section 105 of the Communications Assistance for Law Enforcement Act that require common carriers to" among other things, maintain appropriate policies and procedures.<sup>60</sup> We are persuaded by commenters who express concern that many of our proposals to ensure that carriers establish appropriate policies and procedures for the supervision and control of their personnel exceed the scope of CALEA's mandate and are unduly burdensome.<sup>61</sup> However, we are also sensitive to the FBI's contention that specific carrier personnel policies and procedures are required because "any carrier activities that threaten to compromise the security of surveillance activities could endanger lives and impede prosecutions."<sup>62</sup>

20. Decision. We therefore replace much of our proposed regulatory scheme with a minimum set of requirements intended to allow carriers to develop their own policies and procedures that assure the maintenance of their systems security and integrity in compliance with section 105 of CALEA and section 229(b)(1) of the Communications Act. We conclude that section 105 of CALEA, together with section 229(b)(1) of the Communications Act, requires telecommunications carriers to establish policies and procedures that ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.<sup>63</sup> Specifically, pursuant to section 229(b)(1) of the Communications Act, carriers must ensure that the policies and procedures which they establish for the supervision and control of their officers and employees: (1) require appropriate authorization to activate interception of communications or access to call-identifying information and (2) prevent any such interception or access without such authorization.<sup>64</sup> Finally, we affirm the tentative conclusion we reached in the NPRM and we find that the regulations we prescribe herein apply to all telecommunications carriers as that term is defined in section 102(8) of CALEA.<sup>65</sup>

21. 229(b)(1) - Establish Policies for Employee Supervision and Control. The majority of commenters inform us that our proposals to ensure supervision and control of authorized employees by requiring carriers (1) to designate and list specific employees and officers to assist law enforcement officials in implementing lawful interceptions,<sup>66</sup> (2) to include a statement in carriers' policies and

---

<sup>60</sup> 47 U.S.C. § 229(b).

<sup>61</sup> See, e.g., AT&T Comments at 36-37; BAM Comments at 4; Paging Network, Inc. (PageNet) Comments at 6-7; USTA Comments at 1-2.

<sup>62</sup> FBI Comments at 18-19.

<sup>63</sup> 47 U.S.C. § 1004; 47 U.S.C. § 229(b).

<sup>64</sup> 47 U.S.C. § 229(b).

<sup>65</sup> See NPRM at ¶ 38.

<sup>66</sup> *Id.* at ¶¶ 30, 33.

procedures that only designated employees or officers may participate in lawful interception activities,<sup>67</sup> (3) to permit non-designated employees to effectuate surveillance work only when they do such work unknowingly,<sup>68</sup> and (4) to have designated employees create separate records containing electronic surveillance information for the purpose of guaranteeing the effective supervision of electronic surveillance work performed by non-designated employees,<sup>69</sup> are administratively impractical and burdensome.<sup>70</sup> SBC states that it employs several individuals to perform an interception and that this interception duty is often only a small part of the job function of these employees.<sup>71</sup> SBC believes that to attempt to limit interception activities to a few designated individuals "would cause undue delays in the effectuation of the surveillance, since it would no longer be possible to assign various steps of the process to the most readily available employees."<sup>72</sup> Moreover, BellSouth contends that the geographic dispersion of qualified employees and the incidence of employee turnover or absence does not permit a carrier to limit wiretapping work to only select employees.<sup>73</sup> Furthermore, AT&T argues that such rules are unnecessary because any employee that conducts unauthorized interceptions would be terminated and could face civil or criminal prosecution.<sup>74</sup> Most commenters also opposed our proposed adoption of a rule that requires carriers to create and make available to law enforcement officials upon request a record of each designated employee's name, personal identifying information, official title, and contact numbers.<sup>75</sup> They maintain that such information is invasive to carrier personnel and may compromise the very confidentiality that CALEA and Title 18 seek to protect.<sup>76</sup>

22. Several commenters propose that, instead of being required to create and submit lists of designated and non-designated employees who participate in surveillance work, carriers should only be

---

<sup>67</sup> *Id.* at ¶ 27.

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*

<sup>70</sup> AirTouch Comments at 24; AT&T Comments at 32; BAM Comments at 7; BellSouth Comments at 11; SBC Comments at 19-20; U S West Comments at 23-24; GTE Reply Comments at 8.

<sup>71</sup> SBC Comments at 19.

<sup>72</sup> *Id.* at 19-20.

<sup>73</sup> BellSouth Comments at 11. *See also* SBC Comments at 20.

<sup>74</sup> AT&T Comments at 32; AT&T Reply Comments at 7-10.

<sup>75</sup> NPRM at ¶ 33. *See, e.g.* AT&T Comments at 36; BellSouth Comments at 13; Center for Democracy and Technology (CDT) Comments at 16; CTIA Comments at 26; GTE Comments at 9; PageNet Comments at 9; Powertel, Inc. (Powertel) Comments at 4; SBC Comments at 20, 23; USTA Comments at 7.

<sup>76</sup> *See, e.g.* AT&T Comments at 36; BellSouth Comments at 13; CDT Comments at 16; CTIA Comments at 26; GTE Comments at 9; Powertel Comments at 4; SBC Comments at 20; U S West Comments at 24-25; GTE Reply Comments at 9.

required to appoint a senior officer or employee responsible for effectuating requests for the interception of communications or access to call-identifying information and that employee's contact information.<sup>77</sup>

23. In contrast, the FBI supports our proposal to designate specific employees because it believes this requirement will assist law enforcement authorities in conducting lawful interceptions.<sup>78</sup> However, except in situations where it is impossible for the non-designated employee to infer the nature of his assignment, the FBI does not support our proposal permitting non-designated employees to effectuate certain surveillance work because it strongly believes that, to prevent any possible compromises of security, only specifically designated personnel should be permitted to participate in surveillance work in any way.<sup>79</sup> Also, while the FBI agrees that only designated personnel may create surveillance records, it does not believe that a separate recordkeeping function performed by designated employees would be sufficient to eliminate the concerns posed by the prospect of non-designated employees conducting surveillance functions.<sup>80</sup> The FBI supports the compilation of a confidential list of a core group of designated personnel that must be made available to law enforcement authorities upon request because it believes that such information is important to show a clear chain of custody for the interception when carrier personnel are required to testify in a criminal prosecution.<sup>81</sup> The FBI also seeks to require carriers to have a designated security officer and technical personnel available, either on duty or on call by pager, 24 hours a day, seven days a week to assure that carriers respond promptly to interception orders.<sup>82</sup> The FBI further recommends that, to assure the timeliness of interceptions, carriers should be required to effectuate an interception within 8 hours of receipt of the court order, certification, or consent.<sup>83</sup> In cases of exigent circumstances, the FBI wants carriers to be required to respond within two hours.<sup>84</sup> GTE, however, argues that such effectuation deadlines should not be imposed, and that it is sufficient to require carriers to respond in an expeditious manner consistent with the condition of the network and the needs of customer service.<sup>85</sup>

24. In addition, the FBI recommends that a carrier's policies and procedures should include a background check and trustworthiness determination commensurate with the sensitivity of the activities in which the designated employee will be engaged.<sup>86</sup> The FBI maintains that such background checks are

---

<sup>77</sup> GTE Comments at 9; Omnipoint Comments at 6; U S West Comments at 32.

<sup>78</sup> FBI Comments at 24; FBI Reply Comments at 34.

<sup>79</sup> FBI Comments at 24-25; FBI Reply Comments at 35.

<sup>80</sup> FBI Comments at 26; FBI Reply Comments at 38.

<sup>81</sup> FBI Reply Comments at 37.

<sup>82</sup> FBI Comments at 31-32; FBI Reply Comments at 39, 47.

<sup>83</sup> FBI Comments at 31; FBI Reply Comments at 47.

<sup>84</sup> FBI Comments at 31; FBI Reply Comments at 47.

<sup>85</sup> GTE Reply Comments at 11.

<sup>86</sup> FBI Comments at 19; FBI Reply Comments at 38-39.

consistent with existing carrier practice to supervise personnel handling surveillance work.<sup>87</sup> The FBI further states that the Commission should require carriers to collect this employee information and include it in individual records for all designated personnel because this information would assist law enforcement authorities when a compromise or improper disclosure occurs.<sup>88</sup> CTIA disputes the necessity of such requirements and contends that such collection of information is intrusive to carrier personnel.<sup>89</sup> However, we note that Omnipoint and PCIA state that the FBI should be required to conduct background checks on carrier employees at the carrier's request to assist the carrier in fulfilling its duty to supervise its personnel.<sup>90</sup> Moreover, the FBI contends that, as part of their policies and procedures, carriers should be required to reassign designated employees whose integrity is questioned and to compel designated carrier personnel to execute nondisclosure agreements.<sup>91</sup> Besides ensuring the security of law enforcement authorities, the FBI contends that these procedures would protect carriers from liability in the event an unlawful disclosure occurs because the carrier would be able to demonstrate the existence of clear and specific policies and procedures to safeguard the security of the carrier, law enforcement, and the public.<sup>92</sup> Other commenters, however, contend that such requirements would impinge upon the carrier's discretion over its own employees.<sup>93</sup> We note that SBC states that it would prefer that designated employees only be required to sign a nondisclosure statement, rather than having to complete an affidavit for each interception.<sup>94</sup>

25. Decision. We are persuaded by commenters who state that our proposals to require carriers to make a list of all designated employees and to have separate functions for designated and non-designated employees are administratively impractical. Instead, we conclude that carriers, as part of their policies and procedures, must appoint the senior authorized officer(s) or employee(s) whose job function includes being the point of contact for law enforcement to reach on a daily, around the clock basis. We therefore require carriers to include a description of the job function(s) of such points of contact and a method to enable law enforcement authorities to contact the individual(s) employed in this capacity in their policies and procedures. We decline to adopt the FBI's proposal to require carriers to maintain records of each designated employee's name, personal identifying information, official title, and contact numbers. We conclude that such information is invasive to carrier personnel and could even compromise a carrier's ability to maintain a secure system by identifying the personnel charged with effectuating surveillance functions.

---

<sup>87</sup> FBI Comments at 19.

<sup>88</sup> *Id.*

<sup>89</sup> CTIA Comments at 26.

<sup>90</sup> Omnipoint Comments at 6; Personal Communications Industry Association (PCIA) Comments at 12.

<sup>91</sup> FBI Comments at 20; FBI Reply Comments at 36-37.

<sup>92</sup> FBI Comments at 20.

<sup>93</sup> AT&T Comments at 32; BellSouth Reply Comments at 10.

<sup>94</sup> SBC Comments at 21.

26. Furthermore, we decline to adopt the FBI's recommendations to require carriers to conduct background checks, to reassign personnel in specific situations, and to compel their personnel to sign nondisclosure agreements. While we do not dispute that such practices may ensure a greater level of internal carrier systems security, we believe that carriers will take necessary actions to perform their duty to ensure lawfully authorized interceptions of communications or access to call-identifying information. Also, we decline to require carriers to respond to an interception request within a specific time frame, as suggested by the FBI.<sup>95</sup> We conclude that such a requirement goes beyond the scope of section 105 of CALEA, which addresses the security of intercepts not their implementation. However, we encourage carriers to respond promptly and comply with any other relevant statutes concerning their duty to assist law enforcement authorities to perform an interception of communications or access to call-identifying information.

27. 229(b)(1)(A) - Appropriate Authorization. As we explained above, section 229(b)(1)(A) states that common carriers must establish appropriate personnel supervision and control policies and procedures "to require appropriate authorization to activate interception of communications or access to call-identifying information(.)"<sup>96</sup> Commenters generally agree with our tentative conclusions that section 105 of CALEA imposes a duty upon each carrier to ensure that only lawful interceptions will occur on its premises and that only assigned carrier personnel will perform authorized interceptions.<sup>97</sup> Commenters also do not dispute our finding that the provisions of section 229 of the Communications Act implement the requirements of section 105 of CALEA.<sup>98</sup> Furthermore, commenters support our tentative conclusion that the requirement in section 105 of CALEA that law enforcement present to a carrier appropriate legal authorization to conduct an interception of communications or access to call-identifying information encompasses the provisions of section 2518 of Title 18 of the United States Code.<sup>99</sup>

28. Although some commenters maintain that the term "appropriate authorization" in section 229(b)(1)(A) refers only to the authorization that law enforcement authorities must obtain to conduct an interception,<sup>100</sup> the FBI and Teleport agree with our tentative conclusion that such language also refers to the authorization that a carrier's employee needs from the carrier to engage in the interception activity.<sup>101</sup> In opposing the latter interpretation of "appropriate authorization," CDT and AT&T point to CALEA's

---

<sup>95</sup> FBI Comments at 31.

<sup>96</sup> 47 U.S.C. § 229(b)(1)(A).

<sup>97</sup> NPRM at ¶ 26. Ameritech Operating Companies and Ameritech Mobile Communications, Inc. (Ameritech) Comments at 4; FBI Comments at 18; Sprint Spectrum Comments at 3; AT&T Reply Comments at 21; BellSouth Reply Comments at 4.

<sup>98</sup> NPRM at ¶ 25. Ameritech Comments at 4; AT&T Comments at 28, 32; Sprint Spectrum Comments at 3.

<sup>99</sup> NPRM at ¶ 29. 18 U.S.C § 2518. Section 2518 concerns the procedure that law enforcement must follow to obtain a lawful authorization when seeking to conduct the interception of wire, oral, or electronic communications. FBI Comments at 15; PageNet Comments at 8; SBC Comments at 15.

<sup>100</sup> 360° Communications Company (360°) Comments at 2; Ameritech Comments at 3; AT&T Comments at 30; CTIA Comments at 27; SBC Comments at 9.

<sup>101</sup> NPRM at ¶ 25. FBI Comments at 16; Teleport Communications Group, Inc. (Teleport) Comments at 2.

legislative history and argue that CALEA was not intended to require any generalized changes in carrier practices with respect to operational security of interceptions.<sup>102</sup>

29. Commenters also differ on the standard of scrutiny a carrier must apply in exercising its duty to ensure appropriate authorization of any interception of communications or access to call-identifying information. The FBI recommends that, to protect public safety, "the Commission should specify that the duty of the carrier upon receipt of a facially valid court order or statutorily-based authorization for an intercept extends only to the prompt and good faith implementation of such court orders or authorizations."<sup>103</sup> The FBI further states that, to ensure that an interception is conducted in a timely, secure, and accurate manner, a carrier's review of a court order or certificate of authorization should be limited to whether the document is valid on its face, i.e., whether it is what it purports to be, and whether the interception can technically be implemented.<sup>104</sup> The FBI argues that carriers are not vested with the authority to review the underlying validity and basis for a court order, or authorization in the case of exigent circumstances.<sup>105</sup> The FBI, thus, contends that the Commission should not adopt a rule that carriers include in their internal policies and procedures provisions that would separately define the legal authorizations required for carriers to implement an interception because carrier maintenance of such detailed criteria "could erroneously suggest to carrier personnel that they are entitled to substitute their review for that of a judge" when presented with a facially valid order.<sup>106</sup> In addition, the FBI informs us that the proper basis to determine appropriate authorization should not be limited to 18 U.S.C. § 2518 because additional provisions are contained in federal trap and trace statutes,<sup>107</sup> collateral state statutes,<sup>108</sup> and the Foreign Intelligence Surveillance Act (FISA).<sup>109</sup>

30. Other commenters, however, state that such a limitation on the carrier's duty in ensuring that an interception is lawful would constitute a standard of scrutiny less than that required by 18 U.S.C. § 2520(d) and the legislative history of the Electronic Communications Privacy Act of 1986.<sup>110</sup> Citing to legislative history, CTIA contends that Congress "settled this dispute long ago when it said that a carrier

---

<sup>102</sup> CDT Comments at 15; AT&T Reply Comments at 21.

<sup>103</sup> FBI Comments at 17; FBI Reply Comments at 31.

<sup>104</sup> FBI Comments at 17.

<sup>105</sup> FBI Comments at 16, 22-23; FBI Reply Comments at 30.

<sup>106</sup> FBI Comments at 22; FBI Reply Comments at 31. The FBI states that anecdotal reports exist of instances where carriers have not cooperated with law enforcement authorities even after being presented with a facially valid order because the carrier "did not recognize" a judge's signature or the description of the requested interception service did not precisely match the carrier's official name for that service. FBI Comments at 16; FBI Reply Comments at 30.

<sup>107</sup> 18 U.S.C. § 3121 *et seq.*

<sup>108</sup> *See, e.g.,* D.C. Code Ann. § 23-541 *et seq.* (1981); 18 Pa. Const. Stat. Ann. § 5701 *et seq.* (1983).

<sup>109</sup> 50 U.S.C. § 1801 *et seq.* FBI Comments at 23.

<sup>110</sup> AT&T Reply Comments at 15-17; CTIA Reply Comments at 21.

would be acting in bad faith if it failed to "read the order" or if it "acted beyond the scope of a court order or certification."<sup>111</sup> AT&T states that the Commission should recognize that CALEA specifically requires carriers to protect the privacy of communications not authorized to be intercepted because "Congress intended carriers to do more than blindly implement a surveillance order presented by law enforcement agencies."<sup>112</sup> AT&T also expresses concern that failure to perform this duty might result in carrier liability for violating customers' privacy rights.<sup>113</sup> In response to the FBI's concerns regarding a possible lack of cooperation from carriers, AT&T notes that 18 U.S.C. § 2518(8)(c) grants law enforcement authorities the ability to compel carrier compliance with a court order.<sup>114</sup>

31. Commenters are also divided in regard to our proposal to require carriers to list the exigent circumstances that appear in 18 U.S.C. § 2518(7) in their policies and procedures. The FBI recommends that carriers should not incorporate a list of exigent circumstances in their policies and proposals because a carrier that is presented with certification of emergency circumstances is duty-bound to implement the interception effort and has no right to attempt to discern the factual or legal basis of the statutory emergency.<sup>115</sup> The FBI further states that such a list should not be incorporated because emergency authority and varying exigent circumstances are found in a number of statutes, including 18 U.S.C. §§ 2518(7), 3125, and 50 U.S.C. § 1805(e). In addition, Omnipoint states that this requirement is unnecessary because carriers' compliance obligations under Title 18 already require the carrier's authorized officer or employee to be apprised of the provisions of this statute.<sup>116</sup> Omnipoint also contends that the inclusion of this list would only serve to confuse engineers and non-lawyer personnel.<sup>117</sup> Nevertheless, some carriers support the inclusion of a list of exigent circumstances in the carrier's policies and procedures to assist carrier personnel in performing their duty to ensure only lawfully authorized interception of communications or access to call-identifying information.<sup>118</sup> We note, however, that GTE does not support a requirement to maintain an updated list of exigent circumstances.<sup>119</sup>

32. Decision. We find the explicit language of section 105 of CALEA and section 229(b) of the Communications Act to be dispositive of the issue of whether the reference in section 229 to

---

<sup>111</sup> CTIA Reply Comments at 21 (*citing* to S. Rep. No. 99-541 at 26-27.)

<sup>112</sup> AT&T Reply Comments at 16-17. AT&T states that it is not uncommon for it to receive a wireless surveillance order that contains a subscriber name that does not match the electronic serial number or mobile identification number. *Id.*

<sup>113</sup> AT&T Reply Comments at 18.

<sup>114</sup> 18 U.S.C. 2518(8)(c). AT&T Reply Comments at 15.

<sup>115</sup> FBI Comments at 23.

<sup>116</sup> Omnipoint Comments at 5. Omnipoint states that all the requirements that carriers must follow are found in 18 U.S.C. § 2511(2)(ii)(B). *Id.*

<sup>117</sup> *Id.* at 5.

<sup>118</sup> BellSouth Comments at 12; GTE Comments at 7; Powertel Comments at 6.

<sup>119</sup> GTE Comments at 7.

"appropriate authorization" refers to the authorization that a carrier's employee needs from the carrier to engage in the interception activity.<sup>120</sup> Section 105 of CALEA states that a carrier must ensure that an interception be conducted with the "affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission."<sup>121</sup> Section 229(b) of the Communications Act states that the Commission shall include rules to implement section 105 that require common carriers "to establish appropriate policies and procedures for the supervision and control of its officers and employees."<sup>122</sup> We therefore conclude that the manifest language of these statutory provisions demonstrates Congress's concern that carriers supervise the conduct of their personnel to ensure that any interception of communications or access to call-identifying information is lawfully conducted.

33. Therefore, based on the explicit language of section 105 of CALEA and section 229(b) of the Communications Act, we conclude that "appropriate authorization" refers to both the legal authorization that law enforcement must present to a carrier in the form of an order, warrant, or other authorization issued by a judge or magistrate pursuant to federal or state statutory authority ("appropriate legal authorization") and the authorization a carrier's employee must receive from the carrier to assist law enforcement ("appropriate carrier authorization") to engage in the interception of communication or the access to call-identifying information.<sup>123</sup> We further conclude that a carrier satisfies this requirement in section 229(b)(1)(A) for requiring appropriate authorization when a carrier employee implements the interception of communications or access to call-identifying information only after receiving appropriate legal authorization, and such implementation is in accordance with appropriate carrier authorization. We require that all telecommunications carriers use this comprehensive interpretation of the phrase "appropriate authorization" in their CALEA policies and procedures. In addition, we find that the language in section 229(b)(1)(A) of the Communications Act requiring "appropriate authorization to activate interception of communications or access to call-identifying information[;]" subsumes the requirement in section 105 of CALEA that any interception of call-identifying information can be activated only in accordance with appropriate legal authorization.<sup>124</sup> We thus conclude that the use of the term "lawful authorization" in section 105 of CALEA is encompassed by the term "appropriate authorization" in section 229(b)(1).<sup>125</sup> Therefore, we require carriers to state in their internal policies and procedures that carrier personnel must receive both appropriate legal authorization and appropriate carrier authorization before taking any action to affirmatively implement the interception of communications or access to call-

---

<sup>120</sup> 47 U.S.C § 1004; 47 U.S.C. § 229(b).

<sup>121</sup> 47 U.S.C § 1004.

<sup>122</sup> 47 U.S.C. § 229(b).

<sup>123</sup> 47 U.S.C § 1004; 47 U.S.C. § 229(b).

<sup>124</sup> 47 U.S.C § 1004; 47 U.S.C. § 229(b).

<sup>125</sup> 47 U.S.C § 1004; 47 U.S.C. § 229(b).

identifying information.<sup>126</sup> We note that most carriers support this requirement as part of their policies and procedures.<sup>127</sup>

34. Additionally, we conclude that in order to satisfy sections 105 and 229, a carrier must, upon receipt of a proffered authorization by law enforcement, determine if such authorization is what it purports to be, and whether it can be implemented technically, including that the authorization is sufficiently and accurately detailed to enable the carrier to comply with its terms. We agree with those commenters that contend that sections 105 and 229 require a carrier to review the court order/certification in order to act within its stated scope. We agree with the FBI that neither section 105 nor section 229 vest carriers with the authority to conduct a *de novo* review of the validity of any court order, warrant or other lawful authorization prior to initiating an interception request.<sup>128</sup> We further note that our determination under sections 105 and 229 with regard to the level of scrutiny applicable to a carrier's review of a court order or certification is in no way intended to alter or replace any standard or level of scrutiny imposed under any other state or federal statute (e.g., 18 U.S.C. § 2520(d), the Electronic Communication Privacy Act of 1986) or applicable to any claim for civil liability. Accordingly, we require that, as part of their policies and procedures, carriers should also comply with appropriate authorization requirements contained in any other relevant state or federal statute (i.e., 18 U.S.C. § 2518, federal trap and trace statutes,<sup>129</sup> collateral state statutes, FISA) when reviewing an authorization.<sup>130</sup> To achieve this compliance, we require that carriers ensure that their senior officer(s) or employee(s) responsible for affirmatively intervening to activate the interception of communications or access to call-identifying information is fully apprised of any additional relevant federal and state statutory provisions.

35. Finally, we depart from our proposal to require carriers to include, in their policies and procedures, a current list of the exigent circumstances that appear in 18 U.S.C. § 2518(7) and other collateral state statutes. We believe that this requirement is unnecessary because carriers are already required to be fully apprised of the standard outlined in 18 U.S.C. § 2518(7) and to be able to apply it.<sup>131</sup> Under these circumstances, incorporating the text of the statute into their policies and procedures is unduly burdensome and serves little purpose. Because we are aware that these statutory designations of exigent circumstances may change in the future, we direct the carrier to ensure that its appointed senior officer(s)

---

<sup>126</sup> We note that we modify the rule we proposed in the NPRM to respond to commenters' concerns that it appeared ambiguous and overly broad. See NPRM at ¶ 29 and App. A, § 64.1703. See also AT&T Comments at 29-30. *But see* BellSouth Comments at 10. The rule we adopt states that "carrier personnel must receive appropriate legal authorization and appropriate carrier authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call-identifying information." *Infra*, App. A, § 64.2103(d).

<sup>127</sup> BellSouth Comments at 10.

<sup>128</sup> Ameritech Reply Comments at 4.

<sup>129</sup> 18 U.S.C. § 3121 *et seq.*

<sup>130</sup> 50 U.S.C. § 1801 *et seq.*

<sup>131</sup> See 18 U.S.C. § 2511(2)(ii)(B).

or employee(s) is fully apprised of the different applicable exigent circumstances as part of their job description.

36. 229(b)(1)(B) - Prevention of Unauthorized Interception or Access. The FBI supports our suggestion to require carriers to report to law enforcement authorities and the Commission any security compromises because of the potential threat to the safety of witnesses, undercover agents, and intercept subjects that a compromise could represent.<sup>132</sup> Specifically, the FBI recommends that carriers should be required to report security compromises to the affected law enforcement agencies within two hours and to the Commission every two years.<sup>133</sup> The FBI further recommends that the Commission should develop a standard for determining what preventive measures would be reasonably required by carriers to ensure that compromised interceptions do not go undiscovered or unreported.<sup>134</sup> Commenters generally oppose a requirement to report incidents of compromises and illegal electronic surveillance immediately to the Commission.<sup>135</sup> Although commenters generally support requiring carriers to report incidents of compromises and illegal electronic surveillance to the affected law enforcement agency, they oppose being required to do so within two hours.<sup>136</sup> BellSouth argues that the FBI has not justified the imposition of this time limit and the Commission should not "attempt to establish a one-size-fits-all standard determining what preventive measures would reasonably be required to ensure that compromised intercepts do not go undiscovered or unreported."<sup>137</sup> The commenters further state that they already have such reporting procedures in place in the event a lawful electronic surveillance is compromised or an illegal electronic surveillance is conducted.<sup>138</sup> Moreover, GTE and NTCA oppose a requirement to report a breach of security to both the Commission and law enforcement authorities because they contend that such reporting is burdensome and could expose carriers to penalties and damages under sections 2511 and 2520 of Title 18.<sup>139</sup>

37. In addition, CDT contends that, consistent with Congress's desire to ensure that CALEA compliance measures adopted within carrier switches will not result in increasing system vulnerability to unauthorized interception, the Commission should assure that carriers have appropriate computer security plans in place.<sup>140</sup> CDT thus recommends that carriers' policies and procedures include authentication

---

<sup>132</sup> NPRM at ¶ 27. FBI Comments at 21; FBI Reply Comments at 44.

<sup>133</sup> FBI Comments at 21; FBI Reply Comments at 44. The FBI states that the filing of reports of security breaches will enable the Commission to exercise more effectively its continuing jurisdiction over CALEA-related matters. *Id.*

<sup>134</sup> FBI Comments at 21.

<sup>135</sup> Ameritech Comments at 5; AT&T Comments at 34; BAM Comments at 4; BellSouth Comments at 10.

<sup>136</sup> Ameritech Comments at 5; SBC Comments at 13-14; BellSouth Reply Comments at 9.

<sup>137</sup> BellSouth Reply Comments at 10.

<sup>138</sup> Ameritech Comments at 5; SBC Comments at 13-14.

<sup>139</sup> GTE Comments at 6-7; National Telephone Cooperative Association (NTCA) Comments at 3.

<sup>140</sup> CDT Comments at 7.

procedures, audit trails, intrusion detection measures, and other standard components of computer security.<sup>141</sup> CDT argues that these measures would be more helpful in assuring carrier systems security, rather than the employee supervision and recordkeeping proposals.<sup>142</sup>

38. **Decision.** We conclude that, pursuant to duties imposed by 18 U.S.C. § 2518 and as part of their policies and procedures, telecommunications carriers must report all acts of unauthorized electronic surveillance that occurred on the telecommunications carriers' premises and any compromises of the carrier's system security and integrity procedures that involve the execution of electronic surveillance to the appropriate law enforcement agency. We, however, decline to impose a specific time frame within which a carrier must report a security breach. Instead, we require carriers to report such breaches within a reasonable period of time and in compliance with any other relevant statutes. We also decline to require carriers to report to the Commission incidents of illegal electronic interceptions and compromises of the confidentiality of a lawful interception.<sup>143</sup> We believe that law enforcement agencies are better suited to respond timely and appropriately to such information. However, as discussed more fully below, we note that carriers must maintain accurate records of any unauthorized interceptions or access to call-identifying information as part of their section 229(b)(2) responsibilities. Furthermore, we agree with CDT that authentication procedures, audit trails, and other intrusion detection measures would also assist carriers in performing its duty to prevent unauthorized interceptions and access. However, we decline to require carriers to implement these measures at this time because we believe that each carrier should be allowed to independently determine the extent of its security needs to comply with the rules we prescribe herein. As discussed more fully below, carriers that violate the rules we prescribe to implement section 105 of CALEA will be subject to the penalties of section 229(d).

### C. Section 229(b)(2) Maintaining Secure and Accurate Records

#### a. Recordkeeping of Interceptions

39. Section 229(b)(2) of the Communications Act requires carriers to maintain secure and accurate records of any interception of communications or access to call-identifying information made with or without appropriate authorization.<sup>144</sup> As noted above, the Commission proposed dual record keeping requirements for carriers to follow, including the execution of an affidavit by each employee of a carrier engaged in an interception activity as well as the maintenance of a separate record for every interception which included the following checklist of information: (1) the telephone number(s) and circuit identification numbers involved; (2) the start date and time of the interception; (3) the stop date and time of the interception; (4) the identity of the law enforcement officer presenting the authorization; (5) the name of the judge or prosecuting attorney signing the authorization; (6) the type of interconnection (*e.g.*, pen register, trap and trace, Title III, FISA); and (7) the name(s) of all telecommunications carrier

---

<sup>141</sup> *Id.* at 8.

<sup>142</sup> *Id.*

<sup>143</sup> NPRM at ¶ 27.

<sup>144</sup> 47 U.S.C. § 229(b)(2).

personnel involved in performing, supervising, and internally authorizing the interception, and all names of those who possessed knowledge of the interception.<sup>145</sup>

40. Commenters oppose the Commission's proposed affidavit requirement. BAM argues that this proposal is burdensome and that the NPRM fails to explain how requiring such an affidavit will allow a carrier to achieve any CALEA objective.<sup>146</sup> Many carriers echo this view and generally reject the requirement of an affidavit on the grounds that the record does not support such an unnecessary, impractical, inefficient, and redundant requirement.<sup>147</sup> GTE adds that, not only does the requirement of an affidavit do nothing to enhance the ability of a carrier to meet its CALEA obligations, it "introduces a meaningless exercise which adds additional costs and, more importantly, time to the process when time may be very scarce."<sup>148</sup> In fact, based on the majority of such comments, even the FBI concedes that "a less stringent means than an affidavit would suffice to show the validity of the implementation of an electronic surveillance."<sup>149</sup>

41. Commenters find the proposal to maintain a separate checklist record for every interception far less objectionable. Several carriers explain that they currently maintain records which incorporate much of the checklist information that the Commission is proposing for inclusion.<sup>150</sup> For instance, GTE notes that, like many other carriers, it chooses to maintain the type of information suggested in the checklist record because such information is "logistically" necessary to manage the actual intercept.<sup>151</sup> Except for recording the time during which the intercept is initiated and/or terminated, Ameritech also maintains this type of records.<sup>152</sup> Moreover, Ameritech recommends that carriers' records should include copies of the legal authorization they receive from law enforcement.<sup>153</sup> SBC agrees, explaining that its existing records for interceptions include the court order or other legal authorization and one or two routine work order documents.<sup>154</sup> Ameritech and SBC note, however, that they do not currently keep

---

<sup>145</sup> NPRM at ¶ 32.

<sup>146</sup> BAM Comments at 7.

<sup>147</sup> USTA Comments at 6; AT&T Comments at 33; Omnipoint Comments at 5; BellSouth Response to Initial Regulatory Flexibility Analysis (BellSouth IRFA Response) at 3; BellSouth Comments at 12; U S West Reply Comments at 14; PrimeCo Reply Comments at 8; USTA Reply Comments at 10-11.

<sup>148</sup> GTE Comments at 8.

<sup>149</sup> FBI Reply Comments at 42.

<sup>150</sup> GTE Comments at 8; Ameritech Comments at 6; SBC Communications Comments at 22; Omnipoint Reply Comments at 2; AirTouch Reply Comments at 17; *but see* AirTouch Reply Comments at 17 n. 52 ("AirTouch cannot agree with the Commission's conclusion that the current rule proposals would allow carriers 'to use their existing practices to the maximum extent possible.'")

<sup>151</sup> GTE Comments at 8.

<sup>152</sup> Ameritech Comments at 6.

<sup>153</sup> *Id.*

<sup>154</sup> SBC Comments at 22.

records on the start and stop date and times for interceptions because, in most instances, they merely open the circuit for law enforcement and have no way of knowing when law enforcement begins or ends the actual interception.<sup>155</sup>

42. Focusing on public safety and evidentiary concerns, the FBI endorses the requirement for carriers to maintain a separate checklist record for every interception.<sup>156</sup> The FBI contends that "carriers should be required to maintain separate records of each electronic surveillance activity, and those records (including FISA-related materials) should be maintained in a separate and secure storage area, access to which should be limited to a small number of designated carrier personnel."<sup>157</sup> In addition to the information that the Commission proposed for inclusion in the checklist record, the FBI suggests that carriers should add the name of the issuing court in the case of a court order because doing so would assist both carriers and law enforcement in retrieving information.<sup>158</sup>

43. Other carriers disagree with the Commission's checklist proposal and consider it to be overly burdensome. AT&T believes such a checklist exceeds any record a carrier might maintain for business purposes.<sup>159</sup> BellSouth and AirTouch argue that CALEA does not require the maintenance of such detailed records.<sup>160</sup> While Omnipoint notes that it already keeps much of the records proposed by the Commission, it suggests that we should allow a single sworn statement which does not require notarization by the employee or officer responsible for the interception activity to satisfy a carrier's record keeping obligations.<sup>161</sup> The FBI, in large part, agrees with this suggestion and notes that "a single certification executed by the security officer in charge, that captures the relevant factual information required by law enforcement would be appropriate and consistent with CALEA."<sup>162</sup> Nevertheless, like commenters above, the FBI also suggests deleting from the proposed checklist the requirement for each record to include information regarding when an interception terminates, because such information is often outside of the knowledge of the carriers' personnel.<sup>163</sup>

44. Decision. In light of the comments we received, we decline to adopt our proposed rules to require both an affidavit and a separate record of all interception of communications or access to call-identifying information. We are persuaded by commenters that our dual record keeping proposals are duplicative and overly burdensome. Accordingly, we find that in order to comply with section 229(b)(2),

---

<sup>155</sup> SBC Comments at 22; Ameritech Comments at 6.

<sup>156</sup> FBI Reply Comments at 39.

<sup>157</sup> *Id.* at 40.

<sup>158</sup> FBI Reply Comments at 40.

<sup>159</sup> AT&T Comments at 34.

<sup>160</sup> BellSouth IRFA Response at 3; AirTouch Comments at 22.

<sup>161</sup> Omnipoint Comments at 5.

<sup>162</sup> FBI Reply Comments at 42.

<sup>163</sup> *Id.*

carriers must maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certification. We require that this certification must include, at a minimum, the following information: (1) the telephone number(s) and/or circuit identification numbers involved; (2) the start date and time of the opening of the circuit for law enforcement; (3) the identity of the law enforcement officer presenting the authorization; (4) the name of the judge or prosecuting attorney signing the authorization; (5) the type of interception of communications or access to call-identifying information (*e.g.*, pen register, trap and trace, Title III, FISA); and (6) the name of the telecommunications carriers' personnel who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under section 229(b)(1). This record shall be signed by the individual who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under section 229(b)(1). This individual will, by his/her signature, certify that the record is complete and accurate. This certification must be compiled either contemporaneously with, or within a reasonable period of time after the initiation of the interception of the communications or access to call-identifying information.

45. Having reached the determination to require only a single certification, we nonetheless agree with AirTouch that it is possible that much of this required checklist information can generally be found in the appropriate legal authorization served upon a carrier. Thus, a carrier may satisfy its record keeping obligation by requiring the individual who is responsible for overseeing the interception of communications or access to call-identifying information, and who is acting in accordance with the carriers' policies established under section 229(b)(1), to sign the certification and append the appropriate legal authorization as well as any extensions that have been granted. This combined record must at a minimum, include all of the information in the above-adopted checklist. Moreover, we conclude that it is the carriers' responsibility to ensure that its records are complete and accurate. We emphasize that a violation of this rule is subject to the penalties of section 229(d), discussed more fully below.

46. We note that we have declined to include information regarding the termination time of an interception as part of our required checklist because we are persuaded by commenters that this information is likely to fall outside of the knowledge of a carrier's personnel. This does not, however, relieve carriers of their duty to carefully follow the termination time parameters of the appropriate legal authorization. We have also modified our NPRM checklist proposal from including the name(s) of all telecommunications carrier personnel involved in performing, supervising, and internally authorizing the interception, and all names of those who possessed knowledge of the interception to the less burdensome requirement of a single name and signature because we agree with AirTouch that our original proposal would cause additional work and would likely result in a repetitive list of the same employees for each interception.<sup>164</sup> Instead, we believe that carriers may meet their record keeping obligation by identifying the individual responsible for overseeing the interception and by having that individual certify, by their signature, that the record is accurate and complies with the carriers' policies and procedures established under section 229(b)(1).

47. We also decline to adopt our proposal to have carriers compile this record within 48 hours of the start of each interception. Instead, we believe that by requiring that each certification be compiled either contemporaneously with or within a reasonable period of time after the initiation of the interception of the communication or access to call-identifying information, carriers have the flexibility they need to

---

<sup>164</sup> AirTouch Comments at 23.

establish their own reasonable practices and procedures for record keeping compliance. In reaching this decision, we rely on comments which express concern that carriers' paperwork burden should not be permitted to impede the timeliness with which intercept requests are implemented.<sup>165</sup> Given that we have greatly reduced carriers' record keeping obligations to a minimum amount of required information, much of which they contend they already maintain, we believe that carriers will be able to compile their certifications either contemporaneously with each intercept or within a reasonable amount of time.

48. Additionally, we are not persuaded by the FBI's recommendation that we should adopt a regulation for telecommunications carriers to provide law enforcement officials with the originals or certified copies of carriers' record for each electronic surveillance by no later than five days following the conclusion of an intercept.<sup>166</sup> We find that the imposition of such a requirement would be duplicative and unduly burdensome. BellSouth explains, however, that such records "can, of course, be provide to law enforcement upon a reasonable request and pursuant to appropriate legal authority."<sup>167</sup> Accordingly, where law enforcement officials require the records maintained by telecommunications carriers for evidentiary purposes, they can follow the appropriate discovery procedures to obtain those records.

#### **b. Record Retention Period**

49. As mentioned above, the NPRM sought comment on the length of time carriers should retain interception records.<sup>168</sup> We noted that 18 U.S.C. § 2518(8)(a) requires a ten year retention by law enforcement authorities of intercepted communications.<sup>169</sup> Commenters, including the FBI, generally state that a ten-year record retention requirement is unnecessary and duplicative of the retention rule presently imposed on law enforcement.<sup>170</sup> Commenters also argue that a ten-year record retention period is expensive to implement.<sup>171</sup> U S West argues that carriers should be allowed to determine their own retention period based on industry custom and practice.<sup>172</sup> AirTouch recommends a three year retention period and explains that it follows this time-frame because there is a two year statute of limitations for civil suits against carriers.<sup>173</sup> Sprint Spectrum proposes a five-year record retention period, stating that such a time

---

<sup>165</sup> FBI Comments at 28; GTE Comments at 8; GTE Reply Comments at 8; USTA Reply Comments at 9; U S West Reply Comments at 8 (stating that the Commission should not add another layer of bureaucratic requirements).

<sup>166</sup> FBI Reply Comments at 41.

<sup>167</sup> BellSouth Comments at 12.

<sup>168</sup> NPRM at ¶ 32.

<sup>169</sup> *Id.*

<sup>170</sup> AirTouch Comments at 24; Ameritech Comments at 6 n.5; BAM Comments at 7; U S West Comments at 31; FBI Reply Comments at 40-41; U S West Reply Comments at 14-15.

<sup>171</sup> Ameritech Comments at 6 n.5; GTE Comments at 8.

<sup>172</sup> U S West Comments at 31; U S West Reply Comments at 14-15.

<sup>173</sup> AirTouch Comments at 24.

frame is consistent with record keeping requirements that carriers already have in place.<sup>174</sup> GTE discourages record retention requirements beyond "reasonable limits."<sup>175</sup>

50. Decision. The plain language of section 229(b)(2) requires carriers to maintain secure and accurate records of any interception of communications or access to call-identifying information. It does not, however, provide any direction regarding how long carriers should retain such records.<sup>176</sup> In establishing a retention period, we are sensitive to commenters' concerns about the cost of retaining records and agree that records should be retained only as long as reasonably necessary to comply with section 229(b)(2). We therefore adopt a two tier record retention requirement. First, we conclude that, in compliance with section 229(b)(2), carriers should maintain records of call-identifying information and unauthorized interceptions for ten years. We choose a ten-year retention period to maintain consistency with the retention period for content information in 18 U.S.C. § 2518(8)(a).<sup>177</sup> We believe this requirement is necessary because the record retention obligation imposed under 18 U.S.C. § 2518(8)(a) is limited to the content of an authorized interception.<sup>178</sup> Neither section 2518(8)(a) nor the federal trap and trace statute<sup>179</sup> provide for the retention of records of call-identifying information. Moreover, section 2518(8)(a) does not encompass the retention of records of unauthorized interceptions.<sup>180</sup> Thus, in order to ensure that records of call-identifying information and unauthorized interceptions are maintained securely and accurately, we will require carriers to maintain records of call-identifying information and unauthorized interceptions (including the content of the unauthorized interception) for ten years. We do not believe a ten-year record retention requirement for call-identifying information will be unduly burdensome on carriers because the quantity of call-identifying information required to be collected under a court order is likely to be substantially less than the full content of a communication. Moreover, we anticipate that carriers' policies and procedures will ensure that a carrier will not experience the occurrence of unauthorized interceptions at a frequency that would make the retention of these records overly burdensome.

51. With regard to the second tier, we decline to set a specific time period for maintaining records relating to the content of an authorized interception. Given the record retention requirement imposed on law enforcement under 18 U.S.C. § 2518(8)(a), we find that imposing a duplicative ten year record retention requirement is unnecessary. Instead, we will require carriers to maintain secure and

---

<sup>174</sup> Sprint Spectrum Comments at 2. Sprint Spectrum notes that the Department of Labor requires a record retention period of five years and that financial records are typically retained between three and seven years. *Id.*

<sup>175</sup> GTE Comments at 8.

<sup>176</sup> 47 U.S.C. § 229(b)(2).

<sup>177</sup> 18 U.S.C. §2518(8)(a) requires the "contents of any wire, oral or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. . . [The recordings] shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years."

<sup>178</sup> 18 U.S.C. § 2518(8)(a).

<sup>179</sup> 18 U.S.C. § 3121 *et seq.*

<sup>180</sup> 18 U.S.C. § 2518(8)(a).

accurate records of the content of each authorized interception of communications for a period of time determined by them in accordance with the policies and procedures that they establish under section 229(b)(1) of the Communications Act and applicable state and federal statutes of limitation. As part of the policies and procedures that are submitted to the Commission for review, carriers must include a detailed description of how long they will maintain their records of intercept content. Further, the time period that carriers choose for their individual record retention must have a reasonable justification. Moreover, pursuant to our authority under section 229(c) of the Communications Act, we will modify any carrier's policy or procedure that we determine does not comply with our regulations.<sup>181</sup>

#### D. Sections 229(b)(3) and 229(c): Submission and Review of Policies and Procedures

52. Section 229(b)(3) requires common carriers to submit to the Commission the policies and procedures adopted to comply with the requirements established under sections 229(b)(1) and (b)(2).<sup>182</sup> Section 229(c) states that the Commission shall review those policies and procedures and shall order a common carrier to modify any such policy or procedure that the Commission determines does not comply with its regulations.<sup>183</sup> The Commission shall also conduct such investigations as may be necessary to insure compliance by common carriers with the requirements of the regulations prescribed under this section.<sup>184</sup>

53. As stated above, we requested comment on whether the Commission should establish less burdensome filing requirements for small carriers as determined by their annual operating revenues. Many carriers disagree with the Commission's distinction between small and large carriers as the determining factor by which carriers must submit their policies and procedures to the Commission.<sup>185</sup> Alternatively, some carriers argue that all telecommunications carriers should be permitted to take advantage of the streamlined certification procedure proposed for small carriers in the NPRM.<sup>186</sup> Under that proposal, carriers could either file a statement describing their policies and procedures or certify their compliance

---

<sup>181</sup> 47 U.S.C. §229(c).

<sup>182</sup> 47 U.S.C. § 229(b)(3).

<sup>183</sup> 47 U.S.C. § 229(c).

<sup>184</sup> *Id.*

<sup>185</sup> *See, e.g.*, Omnipoint Comments at 7 (arguing that the Commission should treat all carriers the same with regard to their obligations under CALEA); FBI Comments at 32; BellSouth Comments at 14; SBC Comments at 7-8; U S West Comments at 35; GTE Reply Comments at 11. *But see* Teleport Comments at 8 (stating that small carriers should be permitted to file a certification of compliance in lieu of security procedures and policies); NTCA Comments at 4 (supporting the proposal to give small carriers the certification option).

<sup>186</sup> *See, e.g.*, PCIA Comments at 10; USTA Comments at 8; PrimeCo Comments at 7; BellSouth Comments at 14; SBC Comments at 8; 360° Comments at 5; AirTouch Comments at 25; GTE Reply Comments at 12; CTIA Comments at 28; PCIA Reply Comments at 13.

with Commission rules.<sup>187</sup> AirTouch argues, for example, that streamlined procedures promote the public interest because they reduce administrative burden and expense and thereby increase efficiency.<sup>188</sup>

54. Decision. We conclude that the plain language of section 229(b)(3) requires all telecommunications carriers to submit to the Commission the policies and procedures adopted to comply with the requirements established under sections 229(b)(1)-(2). We agree with commenters that CALEA's statutory language does not make a distinction between carriers, based on size, for the purpose of determining who must submit their policies and procedures to the Commission.<sup>189</sup> We are also persuaded by Omnipoint's argument that law enforcement officials consider all electronic surveillance to be important, all telecommunications carriers are equally responsible for cooperating with lawful requests for assistance with interceptions, and therefore all carriers should be required to submit their policies and procedures for Commission review.<sup>190</sup> Accordingly, we depart from our proposal in the NPRM to establish different filing requirements for large and small carriers and conclude that all telecommunications carriers must file their policies and procedures with the Commission regardless of their gross revenues. As noted by the FBI, the integrity and security of interceptions, and the impact that the loss of vital evidence may have on public safety and the successful conduct of criminal prosecutions, is unrelated to size.<sup>191</sup> Some carriers argue that the Commission should ease the administrative burden on all carriers by allowing them to certify that they are in compliance with statutory requirements.<sup>192</sup> While the Commission is sympathetic to this argument and recognizes the administrative burden placed on both carriers and the Commission by section 229(b)(3) and 229(c), we reject this alternative because it is inconsistent with the plain language of the statute.<sup>193</sup> Moreover, as the FBI notes, the Commission may not have enough information, in a certification or a description, to carry out its obligations under section 229(c) to order any necessary modifications and insure that a carrier's policies and procedures comply with Commission rules.<sup>194</sup>

55. Given that most commenters focused on the Commission's request for information regarding whether we should adopt less burdensome filing requirements for small carriers, few commenters discussed what the Commission's obligations are under section 229(c). We conclude, however, that the statute is clear on the procedure the Commission must follow to review the policies and procedures submitted pursuant to section 229(b)(3).<sup>195</sup> Accordingly, the Commission shall review carriers' policies

---

<sup>187</sup> See NPRM at ¶ 35.

<sup>188</sup> AirTouch Comments at 25.

<sup>189</sup> FBI Comments at 32.

<sup>190</sup> Omnipoint Comments at 7.

<sup>191</sup> FBI Comments at 32.

<sup>192</sup> See, e.g., USTA Comments at 8; PrimeCo Comments at 7.

<sup>193</sup> 47 U.S.C. § 229(b)(3).

<sup>194</sup> FBI Comments at 33.

<sup>195</sup> See 47 U.S.C. § 229(c).

and procedures to determine whether they comply with the Commission's rules established pursuant to sections 229(b)(1)-(2).<sup>196</sup> If the Commission determines that a carrier's policies and procedures are non-compliant, the carrier shall modify its policies and procedures in accordance with an order released by the Commission.<sup>197</sup> Finally, the Commission shall conduct investigations as may be necessary to insure compliance by telecommunications carriers with the requirements of rules established by the Commission under sections 229 of the Communications Act and section 105 of CALEA.<sup>198</sup> This approach advances the objectives of CALEA and, as stated above, is consistent with the plain language of section 229(c).

56. We affirm the tentative conclusion reached in the NPRM and we will require that all carriers file their policies and procedures with the Commission within 90 days from the effective date of the Commission's rules adopted in this Report and Order to implement CALEA.<sup>199</sup> Few commenters objected to our 90 day deadline and we believe that this is a sufficient amount of time for carriers to establish and file their policies and procedures in accordance with Commission rules. Most carriers already have such policies and procedures in place,<sup>200</sup> thereby decreasing the amount of time necessary to prepare them in accordance with Commission rules. We also adopt the FBI's suggestion, unchallenged by any commenter, that carriers be required to file their policies and procedures with the Commission no later than 90 days after the effective date of a merger or divestiture in which a carrier becomes the surviving or divested entity. In addition, we extend this 90-day filing requirement to the amendment by a carrier of existing policies and procedures that it has filed.<sup>201</sup> We believe that 90 days is a reasonable amount of time to incorporate any modifications to already existing policies and procedures and file them with the Commission.

57. Furthermore, we decline to adopt Omnipoint's suggestion that the Commission establish its carrier security and recordkeeping policies in a manner that would prevent such sensitive and confidential information from being made publicly available under the Freedom of Information Act (FOIA).<sup>202</sup> While we are aware of the sensitive nature of a carrier's policies and procedures for systems security and integrity, we must evaluate each FOIA request on a case by case basis to determine whether the requested record falls within one of the FOIA exemptions. As such, adoption of a general rule that automatically exempts all such documents from public inspection is inappropriate at this time.

#### E. Section 229(d): Penalties

---

<sup>196</sup> See 47 U.S.C. § 229(c).

<sup>197</sup> *Id.*

<sup>198</sup> *Id.*

<sup>199</sup> See NPRM at ¶ 37. *But see* 360° Comments at 7 (suggesting that 180 days would be a more appropriate time period).

<sup>200</sup> U S West Comments at 34-35; AirTouch Comments at 19-20; BAM Comments at 9; BellSouth Comments at 7-8; GTE Comments at 6-7; 360° Comments at 3; SBC Comments at 17-20; Teleport Comments at 6-7; USTA Comments at 8; CTIA Reply Comments at 19.

<sup>201</sup> FBI Comments at 35.

<sup>202</sup> See Omnipoint Comments at 7.

58. Section 229(d) of the Communications Act states that a violation by an officer or employee of any policy or procedure adopted by a common carrier pursuant to subsection (b), or of a rule prescribed by the Commission pursuant to subsection (a), shall be considered to be a violation by the carrier of a rule prescribed by the Commission pursuant to this Act.<sup>203</sup> As noted above, the NPRM sought comment on the extent to which a telecommunications carrier's duty to conduct only lawfully authorized interceptions extends vicarious criminal and civil liability to a carrier if the carrier's employees are convicted of conducting illegal electronic interceptions.<sup>204</sup> Commenters overwhelmingly disagree with any attempt by the Commission to create new forms of criminal and/or civil liability, vicarious or otherwise, under section 105 of CALEA.<sup>205</sup> While commenters generally agree that they have a responsibility to prevent unlawful interceptions and to enforce policies to prohibit such activity, they note that unless they fail to monitor and enforce such policies, they cannot be held liable for the unlawful acts of their employees.<sup>206</sup>

59. Decision. We agree with commenters that carrier liability for violations of the Commission's rules implementing section 105 of CALEA have been established by Congress under the plain language of section 229(d) and that promulgating rules that would impose additional liability on carriers is inappropriate.<sup>207</sup> As noted by U S West, in the absence of an explicit statutory mandate, the Commission should not take any action that might expand the criminal and/or civil liability of a carrier without having clear evidence that doing so would substantially promote the goals of CALEA.<sup>208</sup> Commenters also note that nothing in the language of CALEA suggests that a carrier's duties under section 105 affect its liability under 18 U.S.C. §§ 2511 and 2520.<sup>209</sup> Moreover, we agree with those commenters who argue that, even assuming the existence of a carrier's vicarious liability for the acts of its employees, a Commission requirement to report illegal wiretaps or compromises of confidentiality to the Commission

---

<sup>203</sup> 47 U.S.C. § 229(d).

<sup>204</sup> See NPRM at ¶ 27.

<sup>205</sup> See, e.g., Ameritech Comments at 4; BellSouth Comments at 8; Sprint Spectrum Comments at 3; Powertel Comments at 6; USTA Comments at 7; SBC Comments at 11; U S West Comments at 44; FBI Comments at 17.

<sup>206</sup> See, e.g., Ameritech Comments at 4; SBC Comments at 12 (stating that the employer can only be held liable if the unlawful act is authorized by the employer).

<sup>207</sup> See BellSouth Comments at 8; see also BAM Comments at 4 (stating that determining vicarious liability is not within the Commission's rulemaking authority under CALEA); Sprint Spectrum Comments at 3 (stating that unlawful interceptions are addressed in 18 U.S.C. § 2511, and civil remedies and criminal penalties for violating §2511 are already prescribed in §§ 2511 and 2520); USTA Comments at 7 (stating that any such liability would have to be determined pursuant to the established principles of agency as well as the statutory requirements of 18 U.S.C. § 2511); PrimeCo Comments at 6; FBI Comments at 17.

<sup>208</sup> U S West Comments at 45; see also NTCA Comments at 3.

<sup>209</sup> See, e.g., U S West Comments at 44; USTA Comments at 7; NTCA Comments at 3.

or law enforcement cannot, without express direction from Congress, operate to alter or modify civil and criminal liabilities that might arise under Title III.<sup>210</sup>

60. We, therefore, decline to adopt any additional rules that extend criminal and/or civil liability, vicarious or otherwise, to a carrier for the violations of section 105 of CALEA and section 229 of the Communications Act. Instead, if a carrier violates the Commission's rules implementing section 105 of CALEA, the Commission shall enforce, pursuant to section 229(d), the penalties articulated in sections 503(b) of the Communications Act and 1.80 of the Commission's rules.<sup>211</sup> We believe that this decision is consistent with the plain language of the statute and is based on sound public policy.<sup>212</sup>

#### IV. PROCEDURAL MATTERS

##### A. Effective Date

61. Background. In the NPRM, we asked for comment on how much time telecommunications carriers would need to comply with Commission system security and integrity regulations promulgated under 47 U.S.C. § 229, and we tentatively concluded that 90 days from the effective date of this Report and Order should be sufficient.<sup>213</sup> Most parties commenting to our 90-day compliance period proposal fell into two categories: (1) carriers that agreed with the compliance period because they already had extensive electronic surveillance policies and procedures in place,<sup>214</sup> and (2) carriers that were concerned that they would need more time to comply, because they lacked either the resources or experience in supporting law enforcement agencies' electronic surveillance requirements.<sup>215</sup> The FBI offered to work with the Commission and develop model policies and procedures for telecommunications carriers to use as a starting point, from which to develop more specific policies and procedures their companies' unique attributes.<sup>216</sup>

---

<sup>210</sup> SBC Comments at 14; NTCA Comments at 3; U S West Comments at 44.

<sup>211</sup> See 47 U.S.C. § 229(d); 47 C.F.R. § 1.8.

<sup>212</sup> Furthermore, we conclude that sections 105 of CALEA and 229 of the Communications Act do not modify the criminal and/or civil liability of a carrier or its employees pursuant to 18 U.S.C. §§ 2511 and 2520, or any other federal, state or local statutes. Finally, we decline to determine whether reporting illegal wiretaps or compromises of confidentiality to the Commission and/or affected law enforcement agency serves to modify or mitigate a carrier's liability under 18 U.S.C. §§ 2511 and 2520 because we find that to do so is outside the scope of our jurisdiction under CALEA.

<sup>213</sup> NPRM at ¶ 37.

<sup>214</sup> See, e.g., SBC Comments at 23.

<sup>215</sup> See, e.g., 360° Comments at 7 (180 days are necessary). *But see* Rural Telecommunications Group (RTG) Comments at 4 (90-day compliance period is moot without section 103 capability standards).

<sup>216</sup> FBI Reply Comments at 50.

62. Discussion. We conclude that 90 days, *from the effective date of this Report and Order*, is sufficient time for telecommunications carriers to comply with CALEA section 105 and Commission regulations under 47 U.S.C. § 229. We have lessened significantly the number and extent of our proposed regulations in response to recommendations by commenting parties, including the FBI, and regard the final regulations as the minimum that will satisfy CALEA. In addition, we will not begin to enforce our CALEA implementation regulations until 90 days from the effective date of this Report and Order.

### **B. Final Regulatory Flexibility Analysis**

63. As required by section 603 of the Regulatory Flexibility Act (RFA), 5 U.S.C. § 603, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the NPRM. The Commission sought written public comments on the proposals in the NPRM, including the IRFA. The Commission's Final Regulatory Flexibility Analysis (FRFA) in this Report and Order conforms to the RFA, as amended by the Contract With America Advancement Act of 1996 (CWAAA), Pub. L. No. 104-121, 110 Stat. 847 (1996).<sup>217</sup>

#### **(1) Need for and Purpose of this Action**

64. This Report and Order responds to the legislative mandate contained in the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.). The Commission, in compliance with 47 U.S.C. § 229,<sup>218</sup> promulgated rules in this Report and Order to ensure the prompt implementation of section 105 of the Communications Assistance for Law Enforcement Act (CALEA). In enacting CALEA, Congress sought to "make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes. . ."<sup>219</sup> Specifically, Congress sought to balance three key policies with CALEA: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."<sup>220</sup>

65. The rules adopted in this Report and Order implement Congress's goal to make clear a telecommunications carrier's duty to cooperate with law enforcement agencies that request lawful electronic surveillance,<sup>221</sup> and to balance the three key policies enumerated above. The objective of the rules adopted in this Report and Order is to implement as quickly and effectively as possible the national

---

<sup>217</sup> Subtitle II of the CWAAA is "The Small Business Regulatory Enforcement Fairness Act of 1996" (SBREFA), codified at 5 U.S.C. § 601 *et. seq.*

<sup>218</sup> 47 U.S.C. § 229.

<sup>219</sup> CALEA, *supra*, at preamble.

<sup>220</sup> H. Rep. No. 103-837 at 23, *reprinted in* 1994 U.S.C.C.A.N. 3489.

<sup>221</sup> CALEA, *supra*, at preamble.

telecommunications policy for telecommunications carriers to support the lawful electronic surveillance needs of law enforcement agencies.

**(2) Summary of the Issues Raised by Public Comments Made in Response to the IRFA**

66. Summary of Initial Regulatory Flexibility Analysis (IRFA). In the NPRM, the Commission performed an IRFA and asked for comments that specifically addressed issues raised in the IRFA.<sup>222</sup> In the IRFA, the Commission found that the rules it proposed to adopt in this proceeding may have a significant impact on a substantial number of small businesses as defined by section 601(3) of the RFA.

67. In the IRFA, we reiterated our proposed rules in the NPRM requiring telecommunications carriers to establish policies and procedures governing the conduct of officers and employees who are engaged in surveillance activity. The proposed rules required telecommunications carriers to maintain records of all interceptions of communications and call identification information. In addition, the proposed rules required telecommunications carriers to execute an affidavit for each electronic surveillance, and maintain a separate record of each electronic surveillance. Furthermore, we sought comment on the length of time telecommunications carriers should retain electronic surveillance records, and noted that 18 U.S.C. § 2518(8)(a) calls for a retention period of ten years for intercepted communications. The proposed rules also required telecommunications carriers to report security breaches (compromises to lawful electronic surveillance and illegal electronic surveillance) to both the Commission and the affected law enforcement agency.

68. In the IRFA we reiterated that our proposed rules required telecommunications carriers classified as Class A companies pursuant to 47 U.S.C. § 32.11 to file individually with the Commission a statement of its processes and procedures used to comply with the systems security rules promulgated by the Commission. Telecommunications carriers classified as Class B companies pursuant to 47 U.S.C. § 32.11 could elect to either file a statement describing their security processes and procedures or to certify that they observed procedures consistent with the security rules promulgated by the Commission. We noted in paragraph 43 of the NPRM that since electronic surveillance capacity and capability requirements are still being developed, it is not possible to predict with certainty whether the costs of compliance will be proportionate between small and large telecommunications carriers.

69. In the IRFA we tentatively concluded that a substantial number of telecommunications carriers, who have been subjected to demands from law enforcement personnel to provide lawful interceptions and call-identifying information for a period time preceding CALEA, already have in place practices for proper employee conduct and recordkeeping. We noted that as a practical matter, telecommunications carriers need such practices to protect themselves from suit by persons who claim they were the victims of illegal surveillance. By providing general guidance regarding the conduct of carrier personnel and the content of records in the proposed regulations, the Commission intended telecommunications carriers to use their existing practices to the maximum extent possible. Thus, in the IRFA, we tentatively concluded that the additional cost to most telecommunications carriers for conforming to the Commission's proposed regulations, should be minimal.

---

<sup>222</sup> NPRM at ¶¶ 54-76.

70. Comments. Only one party filed comments in response to the IRFA,<sup>223</sup> but many parties commented on the Commission's proposed system security and integrity regulations in response to the NPRM.<sup>224</sup> As noted above, the record provided by all of these commenting parties clearly disfavors the amount of recordkeeping proposed by the Commission in the NPRM, and includes numerous suggestions to reduce the amount of paperwork required by the proposed regulations, without jeopardizing statutory compliance. In response thereto, our final regulations reduce significantly the amount of paperwork required of telecommunications carriers. Other parties commented that the Commission should not promulgate any new rules to implement CALEA.<sup>225</sup> As we noted in paragraph 17, *supra*, a plain reading of 47 U.S.C. § 229(b) shows that Congress requires the Commission to promulgate regulations ensuring the system security and integrity of carriers, compelling carriers to submit their CALEA system security and integrity policies and procedures to the Commission, and providing records that prove to the Commission how each telecommunications carrier is complying with the requirements of CALEA section 105. Thus, commentary against any new regulations contradict the plain language of 47 U.S.C. § 229.

### (3) Description and Estimates of the Number of Entities Affected by This Report and Order

71. Consistent with our prior practice, we shall continue to exclude small incumbent LECs from the definition of a small entity for the purpose of this FRFA. Nevertheless, as mentioned above, we include small incumbent LECs in our FRFA. Accordingly, our use of the terms "small entities" and "small businesses" does not encompass "small incumbent LECs." We use the term "small incumbent LECs" to refer to any incumbent LECs that arguably might be defined by SBA as "small business concerns."<sup>226</sup>

72. *Total Number of Telephone Companies Affected.* Many of the decisions and rules adopted herein may have a significant effect on a substantial number of the small telephone companies identified by SBA. The United States Bureau of the Census ("the Census Bureau") reports that, at the end of 1992, there were 3,497 firms engaged in providing telephone services, as defined therein, for at least one year.<sup>227</sup> This number contains a variety of different categories of carriers, including local exchange carriers, interexchange carriers, competitive access providers, cellular carriers, mobile service carriers, operator service providers, pay telephone operators, PCS providers, covered SMR providers, and resellers. It seems certain that some of those 3,497 telephone service firms may not qualify as small entities or small incumbent LECs because they are not "independently owned and operated."<sup>228</sup> For example, a PCS

---

<sup>223</sup> BellSouth IRFA Response.

<sup>224</sup> See, e.g., FBI Comments at 15-35, GTE Comments at 6-10, and Nextel Comments at 14-15.

<sup>225</sup> See, e.g., USTA Comments at 5-6.

<sup>226</sup> See 13 C.F.R. § 121.210 (SIC 4813).

<sup>227</sup> United States Department of Commerce, Bureau of the Census, *1992 Census of Transportation, Communications, and Utilities: Establishment and Firm Size*, at Firm Size 1-123 (1995) (*1992 Census*).

<sup>228</sup> 15 U.S.C. § 632(a)(1).

provider that is affiliated with an interexchange carrier having more than 1,500 employees would not meet the definition of a small business. It seems reasonable to conclude, therefore, that fewer than 3,497 telephone service firms are small entity telephone service firms or small incumbent LECs that may be affected by this Report and Order.

73. *Wireline Carriers and Service Providers.* SBA has developed a definition of small entities for telephone communications companies other than radiotelephone (wireless) companies. The Census Bureau reports that, there were 2,321 such telephone companies in operation for at least one year at the end of 1992.<sup>229</sup> According to SBA's definition, a small business telephone company other than a radiotelephone company is one employing fewer than 1,500 persons.<sup>230</sup> All but 26 of the 2,321 non-radiotelephone companies listed by the Census Bureau were reported to have fewer than 1,000 employees. Thus, even if all 26 of those companies had more than 1,500 employees, there would still be 2,295 non-radiotelephone companies that might qualify as small entities or small incumbent LECs. Although it seems certain that some of these carriers are not independently owned and operated, we are unable at this time to estimate with greater precision the number of wireline carriers and service providers that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 2,295 small entity telephone communications companies other than radiotelephone companies that may be affected by the decisions and rules adopted in this Report and Order.

74. *Local Exchange Carriers.* Neither the Commission nor SBA has developed a definition of small providers of local exchange services (LECs). The closest applicable definition under SBA rules is for telephone communications companies other than radiotelephone (wireless) companies. The most reliable source of information regarding the number of LECs nationwide of which we are aware appears to be the data that we collect annually in connection with the Telecommunications Relay Service (TRS). According to our most recent data, 1,347 companies reported that they were engaged in the provision of local exchange services.<sup>231</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of LECs that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 1,347 small incumbent LECs that may be affected by the decisions and rules adopted in this Report and Order.

75. *Interexchange Carriers.* Neither the Commission nor SBA has developed a definition of small entities specifically applicable to providers of interexchange services (IXCs). The closest applicable definition under SBA rules is for telephone communications companies other than radiotelephone (wireless) companies. The most reliable source of information regarding the number of IXCs nationwide of which we are aware appears to be the data that we collect annually in connection with the *TRS Worksheet*. According to our most recent data, 130 companies reported that they were engaged

---

<sup>229</sup> 1992 Census, *supra*, at Firm Size 1-123.

<sup>230</sup> 13 C.F.R. § 121.201, Standard Industrial Classification (SIC) Code 4812.

<sup>231</sup> Federal Communications Commission, CCB, Industry Analysis Division, *Telecommunications Industry Revenue: TRS Fund Worksheet Data*, Tbl. 1 (Average Total Telecommunications Revenue Reported by Class of Carrier) (Dec. 1996) (*TRS Worksheet*).

in the provision of interexchange services.<sup>232</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of IXCs that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 130 small entity IXCs that may be affected by the decisions and rules adopted in this Report and Order.

76. *Competitive Access Providers.* Neither the Commission nor SBA has developed a definition of small entities specifically applicable to providers of competitive access services (CAPs). The closest applicable definition under SBA rules is for telephone communications companies other than radiotelephone (wireless) companies. The most reliable source of information regarding the number of CAPs nationwide of which we are aware appears to be the data that we collect annually in connection with the *TRS Worksheet*. According to our most recent data, 57 companies reported that they were engaged in the provision of competitive access services.<sup>233</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of CAPs that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 57 small entity CAPs that may be affected by the decisions and rules adopted in this Report and Order.

77. *Operator Service Providers.* Neither the Commission nor SBA has developed a definition of small entities specifically applicable to providers of operator services. The closest applicable definition under SBA rules is for telephone communications companies other than radiotelephone (wireless) companies. The most reliable source of information regarding the number of operator service providers nationwide of which we are aware appears to be the data that we collect annually in connection with the *TRS Worksheet*. According to our most recent data, 25 companies reported that they were engaged in the provision of operator services.<sup>234</sup> Although it seems certain that some of these companies are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of operator service providers that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 25 small entity operator service providers that may be affected by the decisions and rules adopted in this Report and Order.

78. *Wireless (Radiotelephone) Carriers.* SBA has developed a definition of small entities for radiotelephone (wireless) companies. The Census Bureau reports that there were 1,176 such companies in operation for at least one year at the end of 1992.<sup>235</sup> According to SBA's definition, a small business radiotelephone company is one employing fewer than 1,500 persons.<sup>236</sup> The Census Bureau also reported that 1,164 of those radiotelephone companies had fewer than 1,000 employees. Thus, even if all of the

---

<sup>232</sup> *Id.*

<sup>233</sup> *Id.*

<sup>234</sup> *Id.*

<sup>235</sup> 1992 Census, *supra*.

<sup>236</sup> 13 C.F.R. § 121.201, Standard Industrial Classification (SIC) Code 4812.

remaining 12 companies had more than 1,500 employees, there would still be 1,164 radiotelephone companies that might qualify as small entities if they are independently owned and operated. Although it seems certain that some of these carriers are not independently owned and operated, we are unable at this time to estimate with greater precision the number of radiotelephone carriers and service providers that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 1,164 small entity radiotelephone companies that may be affected by the decisions and rules adopted in this Report and Order.

79. *Cellular Service Carriers.* Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to Cellular Service Carriers and to Mobile Service Carriers. The closest applicable definition under SBA rules for both services is for telephone companies other than radiotelephone (wireless) companies. The most reliable source of information regarding the number of Cellular Service Carriers and Mobile Service Carriers nationwide of which we are aware appears to be the data that we collect annually in connection with the *TRS Worksheet*. According to our most recent data, 792 companies reported that they are engaged in the provision of cellular services.<sup>237</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of cellular service carriers that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 792 small entity cellular service carriers that might be affected by the actions and rules adopted in this Report and Order.

80. *Mobile Service Carriers.* Neither the Commission or the SBA has developed a definition of small entities specifically applicable to mobile service carriers, such as paging companies. The closest applicable definition under SBA rules is for radiotelephone (wireless) companies. The most reliable source of information regarding the number of mobile service carriers nationwide of which we are aware appears to be the data that we collect annually in connection with the *TRS Worksheet*. According to our most recent data, 138 companies reported that they were engaged in the provision of mobile services.<sup>238</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of mobile service carriers that would qualify under SBA's definition. Consequently, we estimate that there are fewer than 138 small entity mobile service carriers that may be affected by the decision and rules adopted in this Report and Order.

81. *Broadband Personal Communications Service.* The broadband PCS spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission defined "small entity" for Blocks C and F as an entity that has average gross revenues of less than \$40 million in the three previous calendar years.<sup>239</sup> For Block F, an additional classification for "very small business" was added, and is defined as an entity that, together with its affiliates, has

---

<sup>237</sup> *TRS Worksheet* at Tbl. 1 (Number of Carriers Reporting by Type of Carrier and Type of Revenue).

<sup>238</sup> *Id.*

<sup>239</sup> See Amendment of Parts 20 and 24 of the Commission's rules -- Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap, *Report and Order*, 11 FCC Rcd 7824, 7850 (1996); see also 47 CFR § 24.720(b).

average gross revenues of not more than \$15 million for the preceding three calendar years.<sup>240</sup> These regulations defining "small entity" in the context of broadband PCS auctions have been approved by SBA.

No small businesses within the SBA-approved definition bid successfully for licenses in Blocks A and B. There were 90 winning bidders that qualified as small entities in the Block C auctions. A total of 93 small and very small business bidders won approximately 40% of the 1,479 licenses for Blocks D, E, and F.<sup>241</sup> However, licenses for Blocks C through F have not been awarded fully, therefore there are few, if any, small businesses currently providing PCS services. Based on this information, we conclude that the number of small broadband PCS licenses will include the 90 winning C Block bidders and the 93 qualifying bidders in the D, E, and F blocks, for a total of 183 small PCS providers as defined by the SBA and the Commission's auction rules.

82. *SMR Licensees.* Pursuant to 47 C.F.R. § 90.814(b)(1), the Commission has defined "small entity" in auctions for geographic area 800 MHz and 900 MHz SMR licenses as a firm that had average annual gross revenues of less than \$15 million in the three previous calendar years. This definition of a "small entity" in the context of 800 MHz and 900 MHz SMR has been approved by the SBA.<sup>242</sup> The rules adopted in this Report and Order may apply to SMR providers in the 800 MHz and 900 MHz bands that either hold geographic area licenses or have obtained extended implementation authorizations. We do not know how many firms provide 800 MHz or 900 MHz geographic area SMR service pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of less than \$15 million. We assume, for purposes of this FRFA, that all of the extended implementation authorizations may be held by small entities, which may be affected by the decisions and rules adopted in this Report and Order.

83. The Commission recently held auctions for geographic area licenses in the 900 MHz SMR band. There were 60 winning bidders who qualified as small entities in the 900 MHz auction. Based on this information, we conclude that the number of geographic area SMR licensees affected by the rule adopted in this Report and Order includes these 60 small entities. No auctions have been held for 800 MHz geographic area SMR licenses. Therefore, no small entities currently hold these licenses. A total of 525 licenses will be awarded for the upper 200 channels in the 800 MHz geographic area SMR auction. The Commission, however, has not yet determined how many licenses will be awarded for the lower 230 channels in the 800 MHz geographic area SMR auction. There is no basis, moreover, on which to estimate how many small entities will win these licenses. Given that nearly all radiotelephone companies have fewer than 1,000 employees and that no reliable estimate of the number of prospective 800 MHz licensees can be made, we assume, for purposes of this FRFA, that all of the licenses may be awarded to small entities who, thus, may be affected by the decisions adopted in this Report and Order.

---

<sup>240</sup> *Id.* at ¶ 60.

<sup>241</sup> FCC News, *Broadband PCS, D, E and F Block Auction Closes*, No. 71744 (rel. January 14, 1997).

<sup>242</sup> See Amendment of Parts 2 and 90 of the Commission's Rules to Provide for the use of 200 Channels Outside the Designated Filing Areas in the 896-911 MHz and the 935-940 MHz Bands Allotted to the Specialized Mobile Radio Pool, PR Docket No. 89-583, *Second Order on Reconsideration and Seventh Report and Order*, 11 FCC Rcd 2639, 2693-702 (1995); Amendment of Part 90 of the Commission's Rules to Facilitate Future Development of SMR Systems in the 800 MHz Frequency Band, PR Docket No. 93-144, *First Report and Order, Eighth Report and Order, and Second Further Notice of Proposed Rulemaking*, 11 FCC Rcd 1463 (1995).

84. *Resellers.* Neither the Commission nor SBA has developed a definition of small entities specifically applicable to resellers. The closest applicable definition under SBA rules is for all telephone communications companies. The most reliable source of information regarding the number of resellers nationwide of which we are aware appears to be the data that we collect annually in connection with the TRS. According to our most recent data, 260 companies reported that they were engaged in the resale of telephone services.<sup>243</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of resellers that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 260 small entity resellers that may be affected by the decisions and rules adopted in this Report and Order.

85. *Pay Telephone Operators.* Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to pay telephone operators. The closest applicable definition under SBA rules is for telephone communications companies other than radiotelephone (wireless) companies. The most reliable source of information regarding the number of pay telephone operators nationwide of which we are aware appears to be the data that we collect annually with the *TRS Worksheet*. According to our most recent data, 271 companies reported that they were engaged in the provision of pay telephone services.<sup>244</sup> Although it seems certain that some of these carriers are not independently owned and operated, or have more than 1,500 employees, we are unable at this time to estimate with greater precision the number of pay telephone operators that would qualify as small business concerns under SBA's definition. Consequently, we estimate that there are fewer than 271 small entity pay telephone operators that may be affected by the decisions and rules adopted in this Report and Order.

86. *Cable Services or Systems.* SBA has developed a definition of small entities for cable and other pay television services, which includes all such companies generating \$11 million or less in revenue annually.<sup>245</sup> This definition includes cable systems operators, closed circuit television services, direct broadcast satellite services, multipoint distribution systems, satellite master antenna systems and subscription television services. According to the Census Bureau, there were 1,788 such cable and other pay television services and 1,439 had less than \$11 million in revenues.<sup>246</sup>

87. The Commission has developed its own definition of a small cable system operator for the purposes of rate regulation. Under the Commission's Rules, a "small cable company" is one serving fewer than 400,000 subscribers nationwide.<sup>247</sup> Based on our most recent information, we estimate that

---

<sup>243</sup> *TRS Worksheet* at Tbl. 1.

<sup>244</sup> *Id.*

<sup>245</sup> 13 C.F.R. § 121.201, SIC Code 4841.

<sup>246</sup> *1992 Economic Census Industry and Enterprise Receipts Size Report*, Table 2D, SIC 4841 (U.S. Bureau of the Census data under contract to the Office of Advocacy of the U.S. Small Business Administration).

<sup>247</sup> 47 C.F.R. § 76.901(e). The Commission developed this definition based on its determination that a small cable system operator is one with annual revenues of \$100 million or less. Implementation of Sections of the 1992 Cable Act: Rate Regulation, *Sixth Report and Order and Eleventh Order on Reconsideration*, 10 FCC Rcd. 7393 (1995).

there were 1,439 cable operators that qualified as small cable system operators at the end of 1995.<sup>248</sup> Since then, some of those companies may have grown to serve over 400,000 subscribers, and others may have been involved in transactions that caused them to be combined with other cable operators. Consequently, we estimate that there are fewer than 1,439 small entity cable system operators that may be affected by the decisions and rules adopted in this Report and Order.

88. The Communications Act also contains a definition of a small cable system operator, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed \$250,000,000."<sup>249</sup> The Commission has determined that there are 61,700,000 subscribers in the United States. Therefore, we found that an operator serving fewer than 617,000 subscribers shall be deemed a small operator, if its annual revenues, when combined with the total annual revenues of all of its affiliates, do not exceed \$250 million in the aggregate.<sup>250</sup> Based on available data, we find that the number of cable operators serving 617,000 subscribers or less totals 1,450.<sup>251</sup> We do not request nor do we collect information concerning whether cable system operators are affiliated with entities whose gross annual revenues exceed \$250,000,000,<sup>252</sup> and thus are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act. We further note that recent industry estimates project that there will be a total of 65,000,000 subscribers, and we have based our fee revenue estimates on that figure.

89. *Other Pay Services.* In the IRFA, we included a category entitled "other pay services."<sup>253</sup> Other pay services are also classified under SIC 4841, which include cable operators, closed circuit television services, direct broadcast satellite services (DBS), multipoint distribution systems (MDS), satellite master antenna systems (SMATV), and subscription television services. We received no comments regarding service providers in this category in response to either the IRFA or the NPRM at large. Accordingly, we cannot determine at this time the number of service providers in this category that intend to offer services to the public as telecommunications carriers, and become subject to CALEA's requirements.

#### **(4) Summary Analysis of the Projected Reporting, Recordkeeping and Other Compliance Requirements and Steps Taken to Minimize the Significant Economic**

---

<sup>248</sup> Paul Kagan Associates, Inc., *Cable TV Investor*, Feb. 29, 1996 (based on figures for December 30, 1995).

<sup>249</sup> 47 U.S.C. § 543(m)(2).

<sup>250</sup> 47 C.F.R. § 76.1403(b).

<sup>251</sup> Paul Kagan Associates, Inc., *Cable TV Investor*, *supra*.

<sup>252</sup> We receive such information on a case-by-case basis only if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to 47 C.F.R. § 76.1403(b).

<sup>253</sup> NPRM at ¶ 72.

**Impact of this Report and Order on Small Entities, Including Significant Alternatives Considered and Rejected.**

90. In this section of the FRFA, we analyze the projected reporting, recordkeeping, and other compliance requirements that may apply to small entities as a result of this Report and Order. We also describe the steps taken to minimize the economic impact of our decisions on small entities, including the significant alternatives considered and rejected.

91. In the final regulations, we affirm our proposal in the NPRM to establish regulations that are general in nature and provide as guidance, so that telecommunications carriers may utilize their existing policies and procedures to the greatest extent possible. In addition, we eliminated all references to proposed rules and tentative conclusions relating to vicarious liability arising out of a telecommunications carrier's failure to accomplish either of CALEA section 105's two objectives.

92. In the final regulations, we eliminated all regulations originally proposed pursuant to 47 U.S.C. § 229(b)(1) that appeared to go beyond the scope of CALEA section 105, overlapped other proposed regulations, were unnecessarily cumbersome, or otherwise unnecessary. Accordingly, carriers must: 1) appoint a senior officer or employee as point of contact responsible for affirmatively intervening to ensure that interception of communications or access to call-identifying information can be activated only in accordance with the appropriate legal authorization; 2) include a description of the job function of the appointed point of contact for law enforcement to reach on a daily, around the clock basis in their policies and procedures; 3) effectuate a requested interception promptly; 4) incorporate our interpretation of the phrase "appropriate authorization" in their policies and procedures; 5) state in their policies and procedures that carrier personnel must receive appropriate legal authorization, before enabling law enforcement officials to implement the interception of communications or access to call-identifying information; 6) require the appointed senior point of contact to be apprised of all relevant federal and state statutory provisions concerning the lawful interception of communications or access to call-identifying information; 7) report security compromises and unlawful interception of communications or access to call-identifying information to the appropriate law enforcement authorities within a reasonable length of time after discovery; 8) maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certification; 9) maintain secure and records of call-identifying information and unauthorized interceptions (including the content of the unauthorized interception) for ten years; 10) maintain secure and accurate records of the content of each authorized interception of communications for a period of time determined by them in accordance with the policies and procedures that they establish under section 229(b)(1) of the Communications Act and applicable state and federal statutes of limitation; 11) provide a detailed description of how long it will maintain its records of intercept content; and 12) file with the Commission, within 90 days of the effective date of these rules, the policies and procedures it uses to comply with the requirements of this subpart, and thereafter, within 90 days of a carrier's merger or divestiture or a carrier's amendment of its existing policies and procedures.

93. We eliminated the requirement of "designated employees," and the requirement for telecommunications carriers to provide updated lists of designated employees that included personal information about them, to law enforcement agencies. Instead, telecommunications carriers, as part of their policies and procedures, should only appoint a senior authorized officer or employee as a point of contact for law enforcement to reach on a daily, around the clock basis. Telecommunications carriers will

include a description of the job function of the designated point of contact and a method to enable law enforcement authorities to contact the individual employed in this capacity in their polices and procedures.

94. We eliminated the proposed regulation requiring a separate affidavit and a separate record for each surveillance. Instead, our final regulation requires that telecommunications carriers compile and maintain a single record of each intercepted communications or access to call-identifying information, certified by a carrier employee in charge of that electronic surveillance, that contains the following information: 1) the telephone number(s) and/or circuit identification number(s) involved; 2) the start date and time of the opening of the circuit for law enforcement; 3) the identity of the law enforcement officer presenting the authorization; 4) the name of the judge or prosecuting attorney who signed the authorization; 5) the type of intercepted communications or access to call-identifying information; 6) the name(s) of the telecommunications carriers' personnel who are responsible for overseeing the interception of communications or access to call-identifying information and who are acting in accordance with the carriers' policies and procedures established under 47 U.S.C. § 229(b)(1). This record shall be signed by the individual who is responsible for overseeing the interception of communications or access to call-identifying information and who is acting in accordance with the carriers' policies and procedures established under 47 U.S.C. § 229(b)(1). To avoid duplicating the existing ten year record retention requirement for records of authorized interception content in 18 U.S.C. § 2518(8)(a), we allow telecommunications carriers to retain records of the content of authorized interceptions for a period of time that they find reasonably necessary. However, because 18 U.S.C. § 2518(8)(a) does not encompass records of call-identifying information and records of unauthorized interceptions, we require carriers to maintain secure and records of call-identifying information and unauthorized interceptions (including the content of the unauthorized interception) for ten years.

95. In the final regulations, we did not affirm our proposal to provide a lessened reporting requirement for carriers that fell below the gross annual revenue threshold established in 47 C.F.R. § 32.9000 of the Commission's rules. As noted above, we conclude that 47 U.S.C. §§ 229(b)(3) requires all telecommunications carriers to submit their policies and procedures to the Commission established under 47 U.S.C. §§ 229(b)(1) and (2). As noted on the record above, the statute makes no distinction between classes of telecommunications carriers for the purpose of lessening the regulatory burden for smaller carriers. Accordingly, our final regulations contain the requirement that all telecommunications carriers must file their system security and integrity policies and procedures with the Commission, within 90 days of this Report and Order's effective date. We note, however, that since the proposed regulations have been drastically reduced, the burden imposed by the regulations adopted herein is also significantly reduced for all telecommunications carriers, including the smaller ones.

#### **(5) Report to Congress**

96. The Commission shall send a copy of this FRFA, along with this Report and Order, in a report to Congress pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996, 5 U.S.C. § 801(a)(1)(A). A copy of this FRFA will also be published in the Federal Register.

#### **C. Paperwork Reduction Act of 1995 Analysis**

97. This Report and Order contains a modified information collection, which has been submitted to the Office of Management and Budget for approval. As part of our continuing effort to

reduce paperwork burdens, we invite the general public to take this opportunity to comment on the information collection contained in this Report and Order, as required by the Paperwork Reduction Act of 1995, Pub. L. No. 104-13. Public comments should be submitted to OMB and the Commission, and are due thirty days from publication of this Report and Order in the Federal Register. Comments should address: (a) whether the proposed collection of information is necessary for the performance of the proper functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology.

#### IV. ORDERING CLAUSES

98. Accordingly, IT IS ORDERED that, pursuant to sections 4(i), 4(j), and 229 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), and 229, and section 105 of the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1004, the rules specified in Appendix A are adopted.

99. IT IS FURTHER ORDERED that the rules set forth in Appendix A WILL BECOME EFFECTIVE 90 days after publication in the Federal Register.

100. IT IS FURTHER ORDERED that the Regulatory Flexibility Analysis, as required by Section 604 of the Regulatory Flexibility Act, and as set forth above is adopted.

101. IT IS FURTHER ORDERED that the Commission's Office of Public Affairs, Reference Operations Division, SHALL SEND a copy of this REPORT AND ORDER, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION



Magalíe Roman Salas,  
Secretary

## APPENDIX A - FINAL RULES

## AMENDMENTS TO THE CODE OF FEDERAL REGULATIONS

## PART 64 - MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Part 64 of the Code of Federal Regulations (C.F.R.) is amended as follows:

1. The authority citation for Part 64 is amended to read as follows:

AUTHORITY: 47 U.S.C. §§ 151, 154, 201, 202, 205, 218-220, and 332 unless otherwise noted. Interpret or apply §§ 201, 218, 225, 226, 227, 229, 332, 48 Stat. 1070, as amended. 47 U.S.C. §§ 201-204, 208, 225, 226, 227, 229, 332, 501 and 503 unless otherwise noted.

2. The table of contents for Part 64 is amended to add Subpart U to read as follows:

**Subpart U - Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act (CALEA)**

§ 64.2100 Purpose.

§ 64.2101 Scope.

§ 64.2102 Definitions.

§ 64.2103 Policies and Procedures for Employee Supervision and Control.

§ 64.2104 Maintaining Secure and Accurate Records.

§ 64.2105 Submission of Policies and Procedures and Commission Review.

§ 64.2106 Penalties.

Part 64 is amended to add Subpart U to read as follows:

§ 64.2100 Purpose.

Pursuant to the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.), this subpart contains rules that require a telecommunications carrier to ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with appropriate legal authorization, appropriate carrier authorization, and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.

§ 64.2101 Scope.

The definitions included in this subpart shall be used solely for the purpose of implementing CALEA requirements.

**§ 64.2102** Definitions.

- (a) **Appropriate Legal Authorization.** The term "appropriate legal authorization" means:
- (1) a court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications; or
  - (2) other authorization, pursuant to 18 U.S.C. § 2518(7), or any other relevant federal or state statute.
- (b) **Appropriate Carrier Authorization.** The term "appropriate carrier authorization" means the policies and procedures adopted by telecommunications carriers to supervise and control officers and employees authorized to assist law enforcement in conducting any interception of communications or access to call-identifying information.
- (c) **Appropriate Authorization.** The term "appropriate authorization" means both appropriate legal authorization and appropriate carrier authorization.

**§ 64.2103** Policies and Procedures for Employee Supervision and Control.

A telecommunications carrier shall:

- (a) establish policies and procedures to ensure the supervision and control of its officers and employees;
- (b) appoint a senior officer or employee as a point of contact responsible for affirmatively intervening to ensure that interception of communications or access to call-identifying information can be activated only in accordance with appropriate legal authorization, and include, in its policies and procedures, a description of the job function of the appointed point of contact for law enforcement to reach on a seven days a week, 24 hours a day basis;
- (c) incorporate, in its policies and procedures, an interpretation of the phrase "appropriate authorization" that encompasses the definitions of "Appropriate Legal Authorization" and "Appropriate Carrier Authorization", as stated above;
- (d) state, in its policies and procedures, that carrier personnel must receive appropriate legal authorization and appropriate carrier authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call-identifying information;
- (e) report to the affected law enforcement agencies, within a reasonable time upon discovery:
  - (1) any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities; and
  - (2) any act of unlawful electronic surveillance that occurred on its premises.
- (f) include, in its policies and procedures, a detailed description of how long it will maintain its records of the content of an interception.

**§ 64.2104** Maintaining Secure and Accurate Records.

A telecommunications carrier shall:

(a) maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certification.

(1) This certification must include, at a minimum, the following information: (i) the telephone number(s) and/or circuit identification numbers involved; (ii) the start date and time of the opening of the circuit for law enforcement; (iii) the identity of the law enforcement officer presenting the authorization; (iv) the name of the person signing the appropriate legal authorization; (v) the type of interception of communications or access to call-identifying information (*e.g.*, pen register, trap and trace, Title III, FISA); and (vi) the name of the telecommunications carriers' personnel who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under § 64.2103 of this subpart.

(2) This certification must be signed by the individual who is responsible for overseeing the interception of communications or access to call-identifying information and who is acting in accordance with the telecommunications carrier's policies established under § 64.2103 of this subpart. This individual will, by his/her signature, certify that the record is complete and accurate.

(3) This certification must be compiled either contemporaneously with, or within a reasonable period of time after the initiation of the interception of the communications or access to call-identifying information.

(4) A telecommunications carrier may satisfy the obligations of subsection (a) of this rule by requiring the individual who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under § 64.2103 of this subpart to sign the certification and append the appropriate legal authorization and any extensions that have been granted. This form of certification must at a minimum include all of the information listed in subsection (a) of this rule.

(b) A telecommunications carrier shall maintain secure and accurate records of:

(1) call-identifying information and unauthorized interceptions (including the content of the unauthorized interception) for ten years;

(2) the content of each authorized interception of communications for a reasonable period of time as determined by the carrier.

(c) It is the telecommunications carrier's responsibility to ensure its records are complete and accurate.

(d) Violation of this rule is subject to the penalties of § 64.2106 of this subpart.

**§ 64.2105** Submission of Policies and Procedures and Commission Review.

(a) Each telecommunications carrier shall file with the Commission the policies and procedures it uses to comply with the requirements of this subpart. These policies and procedures shall be filed with the Federal Communications Commission within 90 days of the effective date of these rules, and thereafter, within 90 days of a carrier's merger or divestiture or a carrier's amendment of its existing policies and procedures.

(b) The Commission shall review each telecommunications carrier's policies and procedures to determine whether they comply with the requirements of § 64.2103 and § 64.2104 of this subpart.

(1) If, upon review, the Commission determines that a telecommunications carrier's policies and procedures do not comply with the requirements established under § 64.2103 and § 64.2104 of this subpart, the telecommunications carrier shall modify its policies and procedures in accordance with an order released by the Commission.

(2) The Commission shall review and order modification of a telecommunications carrier's policies and procedures as may be necessary to insure compliance by telecommunications carriers with the requirements of the regulations prescribed under § 64.2103 and § 64.2104 of this subpart.

**§ 64.2106** Penalties

In the event of a telecommunications carrier's violation of § 64.2103 or § 64.2104 of this subpart, the Commission shall enforce the penalties articulated in 47 U.S.C. § 503(b) of the Communications Act of 1934 and 47 C.F.R. § 1.8 of the Commission's rules.

**APPENDIX B - LIST OF COMMENTERS**Parties Filing Comments

1. AirTouch Communications, Inc. (AirTouch)
2. American Civil Liberties Union (ACLU)
3. Ameritech Operating Companies and Ameritech Mobile Communications, Inc. (Ameritech)
4. AT&T Corporation, and AT&T Wireless Services Inc. (AT&T)
5. Bell Atlantic Mobile, Inc. (BAM)
6. BellSouth Corporation, BellSouth Telecommunications, Inc., BellSouth Cellular Corporation, BellSouth Personal Communications, Inc. and BellSouth Wireless Data, L.P. (BellSouth)
7. Cellular Telecommunications Industry Association (CTIA)
8. Center for Democracy and Technology (CDT)
9. GTE Service Corporation (GTE)
10. National Telephone Cooperative Association (NTCA)
11. Nextel Communications, Inc. (Nextel)
12. Omnipoint Communications, Inc. (Omnipoint)
13. Organization for the Promotion and Advancement of Small Telecommunications Companies (OPASTCO)
14. Paging Network, Inc. (PageNet)
15. Personal Communications Industry Association (PCIA)
16. Powertel, Inc. (Powertel)
17. PrimeCo Personal Communications, L.P. (PrimeCo)
18. Rural Telecommunications Group (RTG)
19. SBC Communications (SBC)
20. Sprint Spectrum L.P. d/b/a Sprint PCS (Sprint)
21. Teleport Communications Group, Inc. (Teleport)
22. United States Cellular Corporation (USCC)
23. United States Department of Justice and Federal Bureau of Investigation (filing jointly) (FBI)
24. United States Telephone Association (USTA)
25. U S West, Inc. (U S West)
26. 360° Communications Company (360°)

Parties Filing Reply Comments

1. AirTouch Communications, Inc. (AirTouch)
2. Ameritech Operating Companies and Ameritech Mobile Communications, Inc. (Ameritech)
3. AT&T Corporation, and AT&T Wireless Services Inc. (AT&T)
4. BellSouth Corporation, BellSouth Telecommunications, Inc., BellSouth Cellular Corporation, BellSouth Personal Communications, Inc. and BellSouth Wireless Data, L.P. (BellSouth)
5. Cellular Telecommunications Industry Association (CTIA)
6. Center for Democracy and Technology (CDT)
7. City of East Ridge Police Department
8. GTE Service Corporation (GTE)
9. Indiana State Police
10. Motorola, Inc. (Motorola)

11. National Technical Investigators' Association
12. New Jersey State Police
13. Nextel Communications, Inc. (Nextel)
14. Office of the Hudson County Prosecutor
15. Omnipoint Communications, Inc. (Omnipoint)
16. Personal Communications Industry Association (PCIA)
17. PrimeCo Personal Communications, L.P. (PrimeCo)
18. SBC Communications (SBC)
19. Telecommunications Industry Association (TIA)
20. Teleport Communications Group, Inc. (TCG)
21. United States Department of Justice and Federal Bureau of Investigation (filing jointly) (FBI)
22. United States Telephone Association (USTA)
23. U S West, Inc. (U S West)