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

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	
	)	

SECOND ORDER ON RECONSIDERATION

Adopted: April 9, 2001 **Released: April 16, 2001**

By the Commission:

I. INTRODUCTION

1. This order resolves two petitions for reconsideration of the *Report and Order*[1] and one petition for reconsideration of the *Second Report and Order,*[2] decisions which implemented sections 102, 105 and 301[3] of the Communications Assistance for Law Enforcement Act (CALEA).[4] We here make minor revisions to sections 64.2103 and 64.2104 of our rules[5] to clarify the arrangements telecommunications carriers subject to CALEA must make to ensure that law enforcement agencies (LEAs) can contact them when necessary, and the interception activity that triggers a record keeping requirement. We make additional clarifications without altering our rules, but otherwise we deny the requests for reconsideration.

2. This order does not consider the technical standards for compliance with the assistance capability requirements of section 103 of CALEA.[6] Those standards, which we addressed in the *Third Report and Order*, are subject to remand from the U.S. Court of Appeals for the D.C. Circuit.[7]

---

[1] Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Report and Order*, 14 FCC Rcd 4151, *recon. sua sponte*, FCC 99-184 (1999) (*Report and Order*).

[2] Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Second Report and Order*, 15 FCC Rcd 7105 (1999) (*Second Report and Order*).

[3] Section 102 sets out definitions of statutory terms. 47 U.S.C. § 1001. Sections 105 and 301 prescribe systems security and integrity (SSI) requirements. 47 U.S.C. §§ 1004, 229. The Commission's SSI rules are codified in Part 64, Subpart V, 47 C.F.R. §§ 64.2100-64.2106.

[4] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

[5] 47 C.F.R. §§ 64.2103 and 64.2104.

[6] Section 103 requires carriers to provide LEAs access to wire and electronic communications and call-identifying information pursuant to a court order or other authorization. 47 U.S.C. § 1002.

[7] Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Third Report and Order*, 14 FCC Rcd 16794 (1999) (*Third Report and Order*); *vacated in part and remanded, United States Telecom Ass'n* (continued….)

II. PETITIONS FOR RECONSIDERATION OF *REPORT AND ORDER*

3. The U.S. Department of Justice and the Federal Bureau of Investigation (FBI) seek reconsideration of the *Report and Order*, which declined to adopt certain of their proposals for personnel security measures, reporting of suspected compromises of systems security, and recording the initiation of intercepts. The FBI also asks us to consider an additional proposal for automated surveillance status messages, which the Commission specifically rejected in the *Third Report and Order*. In addition, the National Telephone Cooperative Association (NTCA) asks for reconsideration or clarification of the rule requiring designation of a point of contact, and reconsideration of the decision not to exempt certain carriers from SSI filing requirements. We will first address the FBI's petition.

A. Personnel Security Measures

4. *Background*. In the *Report and Order*, we adopted requirements that all telecommunications carriers must follow to ensure compliance with the SSI requirements of sections 105 and 301 of CALEA, including certain requirements to ensure supervision and control of authorized employees.[8] We declined to adopt certain other, more detailed requirements proposed by the FBI.[9]

5. In its petition for reconsideration, the FBI calls for "more effective personnel security obligations" than we previously imposed,[10] in order to "ensur[e] the trustworthiness of the private-company employees who have become increasingly responsible for implementing electronic surveillance."[11] It asks that we require carriers to take measures similar to those law enforcement agencies undertake for their employees who conduct interceptions, including:

- Maintaining lists of those employees who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are intercepted. The lists would include their names, dates of birth, social security numbers, and workplace telephone numbers, and would be made available upon request to LEAs.[12]
- Requiring these CALEA-designated employees to sign agreements acknowledging the sensitivity of information involved in electronic surveillance activities, and agreeing not to improperly disclose this information.[13]
- Cooperating with law enforcement as necessary for the completion of limited background checks[14] for employees who are designated to facilitate general criminal intercepts,[15] and

(Continued from previous page)
v. FCC, 227 F.3d 450 (D.C. Cir. 2000). The *Third Report and Order* addressed issues raised when representatives of industry and law enforcement were unable to agree on technical standards for implementing CALEA's assistance capability requirements, and brought their conflicts to the Commission for resolution in accordance with section 107(b) of CALEA, 47 U.S.C. § 1006(b).

[8] *Report and Order*, 14 FCC Rcd at 4158-62.

[9] *See infra* para. 11 and n.37.

[10] FBI petition at 1-2.

[11] FBI reply at 3.

[12] FBI petition at 6-7, reply at 4-8.

[13] FBI petition at 7, reply at 8-10.

[14] "The background checks for employees designated to facilitate general criminal surveillance would normally involve simply a credit check and a criminal records check . . . ." FBI petition at 6.

> more thorough background checks[16] for employees who will facilitate surveillance pursuant to the Foreign Intelligence Surveillance Act (FISA).[17]

6. Opponents generally contend that the Commission sufficiently addressed personnel security obligations in the *Report and Order*, and do not believe there is a need for additional personnel controls.[18] Recognizing their obligations under CALEA to establish appropriate policies and procedures for the supervision and control of their officers and employees, several carriers object to the suggestion they might not be responsible in controlling their own employees or that their employees might present security risks.[19]

7. *Discussion.* After review of the record on reconsideration, we decline to adopt the additional personnel security obligations proposed by the FBI. We find that the detailed statutory requirements, as implemented by our existing rules, should both ensure proper implementation by carriers or authorized interceptions and prevent unauthorized access.

8. We start with a review of the statutory mechanism requiring each carrier to be responsible for ensuring systems security and integrity, and our own set of rules implementing section 301(b). Together, the statute and our existing rules provide ample industry-wide assurance that carriers will establish appropriate policies and procedures to ensure that law enforcement objectives are not compromised. The SSI requirements stem from sections 105 and 301 of CALEA. Section 105 requires 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."[20] Section 301(a) requires us to "prescribe such rules as are necessary to implement the requirements of [CALEA].[21] Section 301(b) mandates that our rules require carriers:

> (1) to establish appropriate policies and procedures for the supervision and control of its officers and employees—
>
> (A) to require appropriate authorization to activate interception of communications or access

(Continued from previous page)

[15] For example, intercepts conducted under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (commonly referred to as Title III intercepts).

[16] "The background checks for employees designated to facilitate FISA [Foreign Intelligence Surveillance Act] surveillance would be more thorough, and would require the designated employees to cooperate directly with the law enforcement agencies conducting the checks by providing references and other necessary information." FBI petition at 6.

[17] FBI petition at 6, reply at 5-6.

[18] *See, e.g.*, Bell Atlantic at 2-3, BellSouth at 5-13, Motorola at 6-7. NTCA sees the list of designated employees as burdensome, unnecessary and invasive. NTCA comments at 5. CTIA argues that non-disclosure agreements would duplicate requirements already contained in court orders and further protected by the possibility of civil and/or criminal penalties. CTIA comments at 4. Only SBC seems to support the FBI's proposals, stating that background checks for designated employees are a "defensible balance" between law enforcement's need for confidentiality and individuals' expectation of privacy, and that non-disclosure agreements are not unreasonable. SBC at 2.

[19] *See, e.g.*, BAM at 5, CTIA at 2, US West at 4. AT&T sees the intent of Section 105 to create a buffer between the LEA and the implementation of an interception or access to call identifying information. AT&T comments at 3. *See also* CTIA comments at 3-4.

[20] 47 U.S.C. § 1004.

[21] 47 U.S.C. § 229(a).

> to call-identifying information; and
> (B) to prevent any such interception or access without such authorization;
> (2) to maintain secure and accurate records of any interception or access with or without such authorization; and
> (3) to submit to the Commission the policies and procedures adopted to comply with the requirements established under paragraphs (1) and (2).[22]

And section 301(c) requires us to review the policies and procedures thus submitted, and to order the modification of any that do not comply with our rules.[23]

9. In the *Report and Order* we adopted the rules mandated by section 301(b). Specifically, section 64.2103 of our rules requires carriers to:

- "Establish policies and procedures to ensure the supervision and control of its officers and employees."[24]
- "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."[25]
- "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 [defined by the Commission]."[26]
- "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."[27]
- Report CALEA security breaches to the affected LEA within a reasonable time upon discovery.[28]
- "Include, in its policies and procedures, a detailed description of how long it will maintain its records of each interception of communications or access to call identifying information . . . ."[29]

Section 64.2104 requires carriers to "maintain a secure and accurate record of each interception of communications or access to call-identifying information," and prescribes the form and content of the

[22] 47 U.S.C. § 229(b).

[23] 47 U.S.C. § 229(c).

[24] 47 C.F.R. § 64.2103(a).

[25] 47 C.F.R. § 64.2103(b).

[26] 47 C.F.R. § 64.2103(c).

[27] 47 C.F.R. § 64.2103(d).

[28] 47 C.F.R. § 64.2103(e).

[29] 47 C.F.R. § 64.2103(f).

required records.[30] Section 64.2105 requires carriers to file with the Commission their SSI policies and procedures, and prescribes Commission review of the filings.[31]

10. Moreover, we are not persuaded that the additional measures the FBI proposes are *necessary* to ensure the security and integrity of CALEA operations and records, as the statute requires.[32] Indeed, the FBI argues only that the proposals would be a useful way for it to oversee carriers' SSI efforts, not that they are *necessary* in order to implement the requirements of CALEA.[33] In the *Report and Order*, consistent with this standard, we adopted "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."[34] The FBI's proposals would depart significantly from this statute-based approach.

11. Further, while the proposals in the FBI's reconsideration petition are somewhat narrower than those it originally made[35] in response to the CALEA *Notice of Proposed Rule Making*,[36] we previously considered and largely declined to adopt such measures in the *Report and Order*.[37] Although it may well be reasonable for carriers to adopt many of the measures advocated by the FBI as part of their SSI policies and procedures,[38] we are not persuaded that they are universally necessary, such that we should impose them as requirements on all carriers. Carriers subject to CALEA range in size from very small to very large, and many have little or no intercept activity. Under these circumstances, imposing the FBI's generic precautionary scheme on all carriers is inconsistent with the Commission's decision to accord carriers substantial discretion to devise SSI policies and procedures they deem appropriate to their particular situations.[39]

12. Finally, the FBI's proposals appear to present practical difficulties as rigid, across-the-board requirements. For example, how often would a background check be required, and what would constitute a

[30] 47 C.F.R. § 64.2104.

[31] 47 C.F.R. § 64.2105.

[32] 47 U.S.C. § 229(a). *See supra* para. 8.

[33] *See, e.g.*, BAM at 2-4. For example, the FBI argues that section 105 calls for a balancing of invasiveness with the need to protect the public from unwarranted searches, and describes its proposals for lists of designated employees and background checks as a means of verifying the trustworthiness of those conducting the surveillance. FBI reply at 4-8.

[34] *Report and Order*, at para. 20.

[35] FBI petition at 5-6, reply at 3.

[36] Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Notice of Proposed Rulemaking*, 13 FCC Rcd 3149 (1997) (*NPRM*).

[37] We declined to require carriers to maintain and provide to LEAs records of each designated employee's name, personal identifying information, official title and contact numbers, concluding that such requirements could be invasive to carrier personnel and could compromise a carrier's ability to maintain a secure system, by identifying personnel charged with effectuating surveillance functions. We also declined to adopt rules concerning mandatory background checks and non-disclosure agreements, determining that carriers would take sufficient measures to ensure the lawful implementation of electronic surveillance without our dictating particular measures. *Report and Order*, at paras. 25-26.

[38] *See, e.g.*, SBC at 2.

[39] For example, it is likely the case that many carriers already designate those employees with intercept responsibilities. *See* FBI petition at 4 n.4, FBI reply at 7. This does not mean, however, that all carriers should formally do so.

sufficient background check? What would constitute an unfavorable check? What would be the result of an unfavorable background check? Would it bar an employee from performing certain job functions, or affect his or her promotion potential? We are concerned that having to promulgate regulations to address these and similar questions could inject the Commission and LEAs into private employment matters to an extent not envisioned by CALEA.

13. We remain confident that carriers will assume the mantle of responsibility assigned to them by CALEA to establish appropriate SSI policies and procedures without micro-management oversight by law enforcement or the Commission. As noted earlier, we ourselves are obligated to review carriers' policies and procedures for compliance with the statute and our regulations.[40] Should we find that a particular carrier's policies and procedures are insufficient to safeguard security and privacy, we will order modifications to that carrier's policies and procedures.[41] Moreover, if the FBI brings to our attention specific problems of a generic nature with carrier implementation of these measures, we will consider amending our rules to address those problems. At this time, however, we do not think the case has been made for more extensive rules in this area.

14. Accordingly, for all the reasons discussed above, we deny the FBI's request that we mandate the personnel security measures listed above. We encourage carriers, however, to consider voluntarily adopting, as internal procedures, measures to respond to the concerns presented by the FBI, as appropriate, and making them part of their SSI policies and procedures.

B. Surveillance Status Message

15. *Background*. The FBI also asks us to require carriers to generate an automated message that would permit LEAs "to confirm periodically that the software used to conduct an interception is working correctly and is accessing the equipment, facilities, or services of the correct subscriber."[42] Information in such a message would include the date, time, and location of the wiretap; identification of the subscriber whose facilities were under surveillance; and identification of all voice channels connected to that subscriber.[43] The FBI argues that the surveillance status message "falls squarely within the mandate of § 105" because it "is specifically designed to minimize . . . unauthorized interceptions, and thus to protect the interests that underlie § 105"[44] by "facilitating the discovery and termination of interceptions that lack lawful authorization."[45]

16. *Discussion*. We find that this proposal suffers the same fundamental infirmity as the FBI's personnel security proposals: the FBI does not argue that surveillance status messages are necessary to ensure systems security and integrity, as CALEA requires,[46] only that they would be useful for LEAs

[40] 47 U.S.C. § 229(c).

[41] *Id.*

[42] FBI petition at 8-9. We note the FBI originally raised this challenge to the Commission's technical standards that were resolved in the *Third Report and Order*, where the Commission determined that the surveillance status message did not fall within section 103 of CALEA.

[43] *Third Report and Order*, at para. 97.

[44] FBI petition at 8.

[45] FBI reply at 14.

[46] 47 U.S.C. 229(a). *See also supra* paras. 8 and 10.

seeking to oversee carriers' SSI activities.[47] Such measures could provide a carrier with an additional means of protection against unauthorized surveillance, and could generate records on authorized surveillance. However, several commenters renew their argument that surveillance status messages would be both technically difficult and costly to implement,[48] an objection the FBI does not here rebut.

17. In considering this proposal, we find that neither the language of section 105 nor the legislative history of CALEA contemplates LEA oversight of carrier SSI measures.[49] Sections 105 and 301(b) of CALEA require carriers to safeguard the security and integrity of their intercept activities, but do not specify how they must do so. As noted previously, we leave decisions about SSI matters to the discretion of carriers, who remain responsible in case of any security breach. We therefore deny the FBI's request that we mandate the use of automated surveillance status messages.[50] As we noted in the *Third Report and Order*, however, "there is nothing that would prevent carriers from providing this capability either on a voluntary basis, or with compensation from LEAs."[51]

C. Reporting Suspected Compromises of System Security

18. *Background*. In response to the CALEA *NPRM*, the FBI proposed that the Commission should adopt a rule requiring carriers to report breaches of systems security within two hours.[52] In the *Report and Order*, we declined to impose a specific reporting time frame. Instead, we decided that carriers must report acts of unauthorized electronic surveillance that occur on their premises and compromises of their SSI procedures involving the execution of electronic surveillance "within a reasonable time upon discovery."[53] The FBI now asks us to modify the rule to require reporting "as soon after discovery as is reasonable in light of privacy and safety concerns and the needs of law enforcement."[54] It maintains that specifying what interests underlie the reasonability standard is necessary so carriers will not "seek to justify substantial delays by reference to an unlimited . . . reserve of 'flexible' . . . explanations," to the detriment of law enforcement.[55]

19. *Discussion*. We share the FBI's concern about the importance of prompt reporting of systems security breaches and expect carriers to exercise their duty to report breaches with due diligence and dispatch. We do not believe, however, that the proposed language would provide appreciably better guidance as to how rapidly a carrier should act in reporting security breaches. We agree with commenters that focusing on only three reasonableness factors ignores others that may be significant in some cases, such as the nature or cause of the breach, the timing of the discovery in relation to the pendency of the

[47] *See, e.g.*, AT&T at 6-8, CTIA at 5-6, WorldCom at 1-2, Motorola at 2-6, PCIA at 2-5, SBC at 2-3, TIA at 2-5, USTA at 3-4. The FBI itself admits that manually checking the status of interceptions "would have essentially the same functionality" as automated surveillance status messages. FBI reply at 14.

[48] *See, e.g.*, BellSouth at 14-15, PCIA at 4-5, TIA at 4-5, US West at 8-9.

[49] *See* AT&T at 7-8.

[50] In light of our disposition of this issue, we need not reach arguments about whether this FBI proposal is properly raised on reconsideration of an order that did not address it in the first place. *See, e.g.*, BellAtlantic at 3-4, CTIA at 5-6, PCIA at 2, TIA at 2, USTA at 3-4, FBI reply at 10-12, US West at 8. *See supra* para. 3.

[51] *Third Report and Order*, at para. 101.

[52] *Report and Order*, at para. 36.

[53] 47 C.F.R. § 64.2103(e). *See Report and Order*, at para. 38.

[54] FBI petition at 9-10.

[55] FBI reply at 15.

intercept (*i.e.*, is the breach discovered during or long after the intercept is in place), the amount of time required to determine whether a suspected breach is in fact a breach, and the amount of time required for the person discovering the breach to report to the carrier's point of contact with law enforcement.[56] Moreover, some commenters contend that the FBI's short list of factors skews the balance of interests to favor law enforcement.[57] Others oppose any attempt to further define "reasonable" as unwarranted because there have not been any problems to date.[58]

20. In the end, absent evidence of significant problems, we prefer to leave the test of reasonableness subject to case-by-case determination. As NTCA points out, if there is a dispute between a carrier and an LEA over the reasonableness of the reporting time, it would be left to a court to resolve the issue of reasonableness, and courts have extensive experience in evaluating a reasonableness standard based on "all relevant and available information, including the needs of law enforcement."[59] We therefore will not adopt additional factors to further define how quickly a carrier should report a security breach to law enforcement.

D. Opening of the Circuit for Law Enforcement

21. *Background*. The FBI also seeks a modification of the Commission's record keeping requirement pertaining to the commencement of interceptions. Section 64.2104(a)(1) of the Commission's rules requires that:

> A telecommunications carrier shall 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 a 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 . . . .[60]

The FBI claims that this language "might be susceptible to an interpretation whereby, if a circuit to law enforcement were to be kept open for the duration of multiple intercepts, the carrier's records of these various intercepts would all show the same 'start date and time,'" rather than recording *individual* interceptions.[61] The FBI asks us to preclude this anomalous result by modifying the phrase "date and time of the opening of the circuit" to read "date and time at which the interception of communications or access to call identifying information was enabled."[62]

22. *Discussion*. This proposal on the part of the FBI drew few comments, and those that were filed reflect some confusion about the FBI's request. We find it reasonable to require a carrier to record the date and time it completes whatever steps are involved in initially establishing LEA access to call information (*i.e.*, call identification information and/or call content) and delivering it to the requesting LEA. We also find it reasonable to require that such information be recorded for each separate telephone number or circuit identification number intercepted, not simply for the activation of a delivery channel that may be

[56] *See, e.g.*, AT&T at 8-9, Bell Atlantic at 4-5, BellSouth at 16, SBC at 3-4.

[57] *See* AT&T at 8-9, NTCA at 8-9, USTA at 4-5, US West at 7.

[58] *See* BellSouth at 15-16, CTIA at 6-7, NTCA at 9.

[59] NTCA at 8-9.

[60] 47 C.F.R. § 64.2104(a)(1).

[61] FBI petition at 11.

[62] FBI petition at 11; FBI reply at 16-17.

used for multiple interceptions.[63] This requirement does not require that a carrier obtain information beyond the ordinary scope of its knowledge, such as when the LEA begins the actual interception,[64] nor does it entail recording the start time of each communication that occurs on an intercepted circuit.[65]

23. AT&T opposes the FBI's request, arguing without explanation that the proposal "would require significant technical modifications to [its] networks and their vendors' equipment—another 'assistance capability' not required by section 103," and would be unnecessary because "carriers routinely maintain, in the ordinary course of business, records necessary to demonstrate good faith compliance with a surveillance order in the event a civil or criminal claim is brought under 18 U.S.C. § 2520."[66] The FBI disputes AT&T's assessment of what the proposal would entail, and maintains that requiring carriers to include in their surveillance records information they already routinely record would not be unduly burdensome.[67]

24. We hereby modify the language of section 64.2104(a)(1) of the rules to require carrier interception certifications to include "the start date and time that the carrier enables the interception of communications or access to call identifying information." This language makes the clarifying change the FBI has requested, but goes further to clarify that the event to be recorded is the carrier's action making the interception available to the LEA. These clarifications do not create a new or additional record keeping requirement beyond what we contemplated in the *Report and Order*, but merely clarify the proper interpretation of this requirement as requested by the FBI. In view of this clarification, we believe AT&T's concern that complying with this requirement would constitute a significant burden is overstated.

E. Point of Contact

25. *Background*. In its Petition for Reconsideration and/or Clarification, NTCA first asks us to clarify an inconsistency it sees between the *Report and Order* and the language of section 64.2103 of the rules, "to make obvious that a single person is not responsible for being law enforcement's point of contact [for CALEA matters], 24 hours a day, 7 days a week."[68]

26. The pertinent portion of the *Report and Order* states:

> [C]arriers . . . 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.

[63] Under section 64.2104(a), a record is required for "*each* interception of communications or access to call-identifying information." 47 C.F.R. § 64.2104(a) (emphasis added).

[64] *See* CTIA comments at 8, SBC comments at 4. Both CTIA and SBC note that carriers are in a position to record information within their knowledge (*e.g.*, when the carrier implements an interception or places a translation in its switch related to the surveillance target). The FBI responds that these commenters' views are consistent with its proposal, in that both "translation" and "implementation" refer to the event the Bureau describes as "enabled." FBI reply at 16-17. *See also* U S West at 7 n.25. *See generally Report and Order*, at paras. 39-48.

[65] As we have noted, federal electronic surveillance laws merely direct carriers to provide the technical assistance necessary to aid law enforcement in making intercepts, not to conduct the intercepts themselves. *See* Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, *Order on Reconsideration*, FCC 99-184, at para. 3.

[66] AT&T at 9-10.

[67] FBI reply at 17.

[68] NTCA petition at 1-2.

> 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.[69]

However, section 64.2103 of the Commission's rules codifies this requirement with the following language:

> A telecommunications carrier shall: . . . (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.[70]

27. *Discussion*. We agree with NTCA that clarification is warranted. The ambiguity arises largely because section 64.2103 combines two somewhat different requirements. Under it, a carrier must: (1) designate someone to be responsible for supervising and controlling its CALEA activities, in order to ensure systems security and integrity, and (2) specify how law enforcement agencies can contact appropriate carrier personnel whenever necessary for CALEA purposes. While the responsible person may also be the primary point of contact, it is impractical for that person to be the *sole* point of contact. As NTCA notes, "No single employee is always available. Employees take vacations, attend seminars and meetings, and are just unavailable."[71] The FBI agrees: "The Department believes that the language and purposes of section 105 can be effectively satisfied in this context as long as each carrier ensures that *someone* is available around the clock to assist law enforcement in the effectuation of lawfully-authorized surveillance, even if the carrier's 'point of contact' is not the same person at all times."[72]

28. We therefore revise section 64.2103 to distinguish these separate requirements, thereby clarifying that a carrier must provide LEAs with round-the-clock access to its CALEA personnel, but not to any one individual. In many cases, for example, the contact information could be a telephone number or numbers that could connect to the duty station(s) of the point(s) of contact during work hours, and could be forwarded so as to page the on-call point(s) of contact outside work hours. Whatever arrangements a particular carrier might make, the objective would be to provide a means for law enforcement to reach responsible carrier personnel with a minimum of delay.

29. We next take this opportunity to clarify on our own motion two other minor issues regarding carrier SSI policies and procedures, which have arisen in our review of initial filings.[73] First, we revise section 64.2103 to require carriers to place their information regarding responsible personnel and contacts in a separate appendix to their SSI policies and procedures, to simplify both extracting this information for LEA use and updating it as changes occur.[74] Carriers whose initial SSI filings include the required personnel and contact information, but not in a separate appendix, need not revise their filings solely to put

---

[69] Report and Order, at para. 25.

[70] 47 C.F.R. § 64.2103(b).

[71] NTCA petition at 3.

[72] FBI comments at 2. PCIA, the only other party commenting on this issue, also supports the NTCA request. PCIA at 5-6.

[73] Section 64.2103 became effective on February 2, 2000, and initial filings were due by May 2, 2000. *See* 65 Fed. Reg. 8666 (Feb. 22, 2000).

[74] For example, when changes occur to contact information, the carrier could simply revise and file the appendix, not the entire policies and procedures document.

the information in an appendix. However, carriers whose initial filings do not include the required information must promptly amend their filings to do so, and should submit it in the form of a separate appendix. Initial and revised filings made after the effective date of the rule changes made herein must include such information in a separate appendix.

30. Second, we clarify that we will routinely make available to law enforcement agencies the carriers' responsible personnel and contact information. This represents a continuation of our current practice, not a change, since contact information that is unavailable to LEAs would obviously serve no purpose. This clarification also resolves one of the requests the FBI makes in the late-filed supplement to its petition, namely that we "state explicitly that . . . contact information will . . . continue to be made available to the federal, state and local law enforcement agencies for whose benefit the information is maintained."[75]

31. Finally, we decline to adopt other FBI proposals set out in its late-filed supplement. The FBI suggests that carriers be required to notify the Commission of "any significant change" in point of contact information, "immediately"[76] and "in writing, or (preferably) by electronic message," and that the Commission specify a form for providing contact information.[77] We find these proposals, like some others discussed above, too inflexible to apply to all carriers. Under the rules, carriers must provide information necessary for LEAs to contact them for purposes of CALEA, and we prefer to leave to their individual discretion how best to update this information in a clear and timely manner. Carriers should keep in mind, however, that the 90-day deadline for filing updated SSI policies and procedures specified in section 64.2105(a) is the *maximum* time in which to file. Where the only change is to the relatively brief appendix identifying responsible personnel and contact information, we would expect carriers to update this information as soon as practical, to ensure that LEAs' ability to contact carriers is not adversely affected. Likewise, we expect carriers to provide the required information clearly, and thus see no need to specify a particular format. Should later experience reveal problems in either clarity or timeliness, we will revisit the need for further regulation.

F. Exemption for Small Businesses

32. *Background*. NTCA next asks us to exempt small, rural telephone companies from the requirement to file with the Commission the policies and procedures they use to comply with the systems security and integrity rules,[78] as required by section 64.2105 of the Commission's rules.[79] NTCA argues here that the filing requirement imposes unnecessary burdens on both carriers and the Commission, and that the possibility of money forfeitures is an adequate tool "to ensure that companies will develop and maintain compliant policies."[80]

33. *Discussion*. In the *Report and Order*, we recognized that this filing requirement would entail some burden on carriers, and considered options for reducing the burden for small carriers. We concluded, however, that "the plain language of section 229(b)(3) requires all telecommunications carriers to submit to

[75] FBI supplement at 3.

[76] Section 64.2105(a) currently requires carriers to file amended SSI policies and procedures within 90 days of either their revision or a triggering event. 47 C.F.R. § 64.2105(a).

[77] FBI supplement at 4-5. AT&T, CTIA and PCIA oppose these proposals. AT&T response at 3-7, CTIA opposition at 3-6, PCI opposition at 2-6.

[78] NTCA petition at 3-4.

[79] 47 C.F.R. § 64.2105(a).

[80] NTCA petition at 3-4.

the Commission the policies and procedures adopted to comply with the requirements established under sections 229(b)(1)-(2)," without "distinction between the carriers, based on size."[81] Only PCIA supports NTCA's proposal, but neither party addresses the statutory barrier to the relief NTCA seeks.[82] As the FBI notes, the NTCA argument "is simply an argument against [the structure of] the statute itself . . . , [which] should be pressed before Congress, not before the Commission."[83] We agree with the FBI's interpretation that the relief NTCA seeks is contrary to the statutory language, and therefore we deny NTCA's request.

34. We would note, however, that section 64.2103 does not prescribe the content or form of a carrier's policies and procedures document. Thus, each carrier has discretion, subject to Commission oversight, to tailor its policies and procedures to its own unique circumstances. This flexibility offers a measure of relief for small carriers whose SSI needs are modest, and makes compliance with section 64.2105 less burdensome for those carriers.

III. PETITION FOR RECONSIDERATION OF *SECOND REPORT AND ORDER*

35. *Background*. In its petition for reconsideration and/or clarification of the *Second Report and Order*, the FBI asks us to clarify carriers' responsibility for CALEA compliance in resale situations. In the *Second Report and Order*, we noted that CALEA's assistance capability requirements apply to "equipment, facilities, *or services* that provide a customer or subscriber with the ability to originate, terminate, or direct communications."[84] The only statutory exceptions to the assistance capability requirements are based on the nature of the service provided: private line services and information services.[85] We therefore held that as telecommunications carriers, resellers are generally subject to all provisions of CALEA. We did, however, find that "resellers' responsibility under CALEA should be limited to their own facilities" and that they are "not . . . responsible for the CALEA compliance responsibilities of the carrier whose services they are reselling with respect to the latter's underlying facilities."[86]

36. The FBI is concerned that law enforcement might be effectively disabled from enforcing CALEA's assistance capability obligations in certain resale situations. In particular, the FBI focuses on instances where a reseller denies CALEA responsibility on the grounds that it does not use its own facilities to provide the service in question, and the underlying facilities-based carrier also denies responsibility arguing that it is not a "telecommunications carrier" under CALEA because it does not provide telecommunications services directly to the public on a "common carrier" basis.[87] The FBI asks that we clarify either that: (1) a carrier that sells telecommunications services to a reseller is itself a "telecommunications carrier" under CALEA with respect to such services; or (2) if an underlying facilities-based service provider is not a "telecommunications carrier," the reseller remains responsible in full for ensuring that the telecommunications services it provides to the public, and the equipment and facilities involved in providing that service, are CALEA-compliant.[88]

---

[81] *Report and Order*, at para. 54.

[82] PCIA at 6.

[83] FBI response and partial opposition at 3.

[84] *Second Report and Order*, at para. 10 (quoting 47 U.S.C. § 1002(a))(emphasis added).

[85] 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2). *See also Second Report and Order*, at para. 12.

[86] *Second Report and Order*, at para. 24.

[87] FBI petition at 1-2.

[88] *Id.* at 3.

37. *Discussion*. We agree with the FBI that Congress intended to ensure that services offered by telecommunications carriers are to comply with the assistance capability requirements of CALEA section 103. We clarify here that the language in the *Second Report and Order* regarding resellers was not intended to thwart that fundamental statutory purpose. As noted above, in the *Second Report and Order* we held that as telecommunications carriers, resellers are generally subject to CALEA. However, exercising our authority under section 102(8)(C),[89] we exempted resellers from those requirements to the extent that they resell services of other, facilities-based carriers. We here clarify that that decision was premised on the obligations of the underlying facilities-based carriers to comply with CALEA. Thus, to the extent that a reseller resells services or relies on facilities or equipment of an entity that is not a telecommunications carrier for purposes of CALEA and thus is not subject to CALEA's assistance capability requirements,[90] we did not intend to exempt the reseller from its overall obligation to ensure that its services satisfy all the assistance capability requirements of section 103.

38. We appreciate that some resellers may face difficulties in making arrangements with their service providers for CALEA assistance capabilities. Yet we do not agree with TRA that simply because non-facilities-based resellers must rely on others for CALEA assistance capabilities, they "could never achieve compliance with CALEA assistance capability obligations," or that doing so "would expose the consuming public generally to the risk of unacceptable rate increases or diminished availability of service offerings."[91] In situations where a reseller does not resell the services of a facilities-based carrier subject to CALEA, it can contract with its facilities provider or third parties for CALEA assistance capabilities in the same way it contracts for any other network capabilities. We expect that CALEA assistance capabilities generally will be available, and the statute offers relief mechanisms where their availability is delayed or not reasonably achievable.[92]

IV. PROCEDURAL MATTERS

A. Motions

39. In the interest of having a full record on these important issues, we will grant the FBI's motions to file a consolidated reply, and for acceptance of the late-filed supplement to its petition, and deny the various oppositions to the latter.

B. Final Regulatory Flexibility Certification

40. The *Report and Order* in this proceeding incorporated a Final Regulatory Flexibility Analysis of the effect on small entities of the CALEA rules adopted at that time,[93] and the *Second Report and Order* incorporated a Final Regulatory Flexibility Analysis of the effect on small entities of the actions taken therein, which did not include CALEA rules.[94] The Regulatory Flexibility Act of 1980, as amended

[89] 47 U.S.C. § 1001(8)(C).

[90] *See Second Report and Order*, at paras. 9-13.

[91] TRA at 5-6.

[92] *See* 47 U.S.C. 1006(c) and 1008(b)(1).

[93] *See* paragraphs 63-95 of the full text of the *Report and Order*. The *Order on Reconsideration* revised these rules and incorporated in Appendix B a Supplemental Regulatory Flexibility Analysis reflecting the impact of the revised rules on small entities.

[94] *See* Appendix B of the full text of the *Second Report and Order*.

(RFA),[95] requires that a regulatory flexibility analysis be prepared for rulemaking proceedings, unless the agency certifies that "the rule will not have a significant economic impact on a substantial number of small entities."[96] The RFA generally defines "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[97] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[98] A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration.[99]

41. This *Second Order on Reconsideration* does not make major revisions to the existing CALEA rules or enact new requirements, but does make minor revisions to sections 64.2103 and 64.2104.[100] First, it clarifies the arrangements that telecommunications carriers subject to CALEA must make to ensure that law enforcement agencies can contact them when necessary, by requiring the use of a "pull-off" page for submitting contact information to the Commission. Second, it clarifies the definition of the interception activity that triggers a record keeping requirement. Neither change requires the collection of additional information or increases the frequency of record keeping, and the cost of complying with these revisions is nominal. Third, it clarifies without rule change that resellers are not exempt from the obligation to ensure that their services satisfy all the assistance capability requirements of section 103 of CALEA. As such, this action imposes no reporting, recordkeeping or other compliance requirement beyond those imposed by CALEA itself. Accordingly, the Commission certifies, pursuant to § 605(b),[101] that the rule revisions adopted in this *Second Order on Reconsideration* will not have a significant economic impact on a substantial number of small entities.

42. The Commission will send a copy of the *Second Order on Reconsideration*, including a copy of this final certification, in a report to Congress pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996.[102] The Commission will also send a copy of the *Second Order on Reconsideration*, including this final certification, to the Chief Counsel for Advocacy of the Small Business Administration, and will publish notice in the Federal Register.[103]

---

[95] The RFA, 5 U.S.C. § 601 *et seq.*, has been amended by the Contract With America Advancement Act of 1996, Pub. L. No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[96] 5 U.S.C. § 605(b).

[97] *Id.* at § 601(6).

[98] *Id.* at § 602(3) (incorporating by reference the definition of "small business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[99] 15 U.S.C. § 632.

[100] 47 C.F.R. §§ 64.2103, 64.2104.

[101] 5 U.S.C. § 605(b).

[102] 5 U.S.C. § 801(a)(1)(A).

[103] 5 U.S.C. § 605(b).

C. Paperwork Reduction Act of 1995 Analysis

43. This Order does not contain a new information collection, but only requires a change of format for future submissions of a carrier's SSI filing. Specifically, as described in paragraph 29, and in conformance with revised section 64.2103(b)(4) of the Commission's rules, 47 C.F.R. § 64.2103(b)(4), point of contact information must appear in a separate appendix attached to the SSI report.

D. Authority

44. This action is taken pursuant to Sections 1, 2, 4(i) and (j), 201, 229, 303(f) and (r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i) and (j), 201, 229, 303(f) and (r), and 332.

E. Further Information

45. For further information, contact John Spencer or Susan Kimmel of the Policy Division, Wireless Telecommunications Bureau, at 202-418-1310 (voice) or 202-418-1169 (TTY).

V. ORDERING CLAUSES

46. Accordingly, IT IS ORDERED that Part 64 of the Commission’s Rules is amended as set forth in Appendix B.

47. IT IS FURTHER ORDERED that the rule amendments made by this Order and specified in Appendix B SHALL BECOME EFFECTIVE 30 days after the date of their publication in the Federal Register.

48. IT IS FURTHER ORDERED that the Consumer Information Bureau, Reference Operations Division, SHALL SEND a copy of this Order, including the Final Regulatory Flexibility Certification, to the Chief Counsel for Advocacy of the Small Business Administration.

49. IT IS FURTHER ORDERED that the DOJ/FBI Motion to File Consolidated Reply to Oppositions to Petition for Reconsideration Exceeding Ten Pages in Length IS GRANTED.

50. IT IS FURTHER ORDERED that the Motion for Acceptance of Supplemental Comments filed by the Department of Justice/Federal Bureau of Investigation IS GRANTED.

51. IT IS FURTHER ORDERED that the Petition for Reconsideration of Section 105 *Report and Order* filed by the Department of Justice/Federal Bureau of Investigation IS GRANTED TO THE EXTENT INDICATED HEREIN, and IS OTHERWISE DENIED.

52. IT IS FURTHER ORDERED that the Petition for Reconsideration and/or Clarification filed by the National Telephone Cooperative Association IS GRANTED TO THE EXTENT INDICATED HEREIN, and IS OTHERWISE DENIED.

53. IT IS FURTHER ORDERED that the Petition for Reconsideration and/or Clarification of the *Second Report and Order* filed by the Department of Justice/Federal Bureau of Investigation IS GRANTED TO THE EXTENT INDICATED HEREIN, and IS OTHERWISE DENIED.

FEDERAL COMMUNICATIONS COMMISSION

Magalie Roman Salas
Secretary

Appendix A
Petitions and Responsive Comments

Petitions:

Department of Justice/Federal Bureau of Investigation (Petition for Reconsideration of Section 105 *Report and Order*)
National Telephone Cooperative Association (NTCA) (Petition for Reconsideration and/or Clarification [of *Report and Order*])
Department of Justice/Federal Bureau of Investigation (Petition for Reconsideration and/or Clarification [of *Second Report and Order*])

Comments and Oppositions:

AT&T Corp.
Bell Atlantic
Bell Atlantic Mobile, Inc. (BAM)
BellSouth Corporation
Cellular Telecommunications Industry Association (CTIA)
Department of Justice/Federal Bureau of Investigation (FBI)
MCI WorldCom, Inc. (WorldCom)
Motorola, Inc.
National Telephone Cooperative Association (NTCA)
Personal Communications Industry Association (PCIA)
SBC Communications
Telecommunications Industry Association (TIA)
Telecommunications Resellers Association (TRA)
United States Telecom Association (USTA)

Reply Comments:

Department of Justice/Federal Bureau of Investigation
U S WEST, Inc.

Supplemental Comments, Oppositions and Replies:

Department of Justice/Federal Bureau of Investigation (supplemental comments; motion for acceptance of supplemental comments and reply to opposition)
AT&T Corp. and AT&T Wireless Group (response)
BellSouth Corporation (opposition)
Cellular Telecommunications Industry Association (opposition)
Personal Communications Industry Association (opposition to motion for acceptance)

Appendix B
Final Rules -- §§ 64.2103, 64.2104

AMENDMENTS TO THE CODE OF FEDERAL REGULATIONS

RULE CHANGES
For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR Part 64 as follows:

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Subpart V – Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act (CALEA)

1. Section 64.2103 is revised to read as follows:

§ 64.2103 Policies and procedures for employee supervision and control.

A telecommunications carrier shall:

(a) Appoint a senior officer or employee responsible for ensuring 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.

(b) Establish policies and procedures to implement sub-paragraph (a) of this paragraph, to include:

(1) a statement 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;

(2) an interpretation of the phrase "appropriate authorization" that encompasses the definitions of appropriate legal authorization and appropriate carrier authorization, as used in sub-paragraph (b)(1);

(3) a detailed description of how long it will maintain its records of each interception of communications or access to call-identifying information pursuant to § 64.2104;

(4) in a separate appendix to the policies and procedures document:

(i) the name and a description of the job function of the senior officer or employee appointed pursuant to sub-paragraph (a); and

(ii) information necessary for law enforcement agencies to contact the senior officer or employee appointed pursuant to sub-paragraph (a) or other CALEA points of contact on a seven days a week, 24 hours a day basis.

(c) 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.

2. Section 64.2104(a)(1)(ii) is revised to read as follows:

§ 64.2104 Maintaining secure and accurate records.

(a) * * * * *

(1) * * * * *

(ii) The start date and time that the carrier enables the interception of communications or access to call identifying information;

* * * * *