CALEA COMPLIANCE MANUAL
FOR

metroPCS inc

Adopted: April 22, 2002

Filed with the Federal Communications Commission: April 22, 2002

Revised 10/3/2006

Table of Contents

metroPCS inc

CALEA Compliance Policy

1.0 OBJECTIVE

It is the policy of MetroPCS to comply with the letter and spirit of all laws of the United States, including the *Communications Assistant for Law Enforcement Act* (hereinafter referred to as "CALEA") relating to the implementation of law enforcement wiretap requests. CALEA requires MetroPCS to implement security measures to safeguard the privacy and reliability of information obtained through lawfully authorized interceptions of communications (i.e., wiretaps, pin registers, and subpoenas) and to help prevent unauthorized interceptions. MetroPCS Personnel must receive appropriate legal authorization and appropriate carrier authorization (as such terms are defined herein) to implement the interception of communications or access to call-identifying information.

2.0 SCOPE

This Policy applies to all employees, contractors, and consultants of MetroPCS and each of its subsidiaries (collectively "MetroPCS Personnel").

3.0 DEFINITIONS

3.1 Appropriate Legal Authorization

The term "Appropriate legal authorization" means:

- A court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications, or
- Other authorization issued pursuant to an appropriate federal or state statute (i.e., Title 18, federal trap and trace statutes, Foreign Intelligence Surveillance Act or any other relevant federal or state statue.).

3.2 Appropriate Carrier Authorization

The term "Appropriate carrier authorization" means the policies and procedures adopted by MetroPCS to supervise and control MetroPCS personnel authorized to assist law enforcement in conducting any interception of communications or access to call identifying information. Compliance with these policies and procedures requires, but is not limited to:

- Verification of appropriate legal authorization (Section 3.1)
- The legal authorization is what it purports to be (i.e., is valid on its face)
- The request is described in sufficient detail such that it can be technically implemented

3.3 Appropriate Authorization

- The term "appropriate authorization" means both appropriate legal authorization and appropriate carrier authorization.

4.0 POLICY

It is MetroPCS' policy that no interception of communications (i.e. wiretaps) or access to call-identifying information using MetroPCS' equipment and/or systems will be activated unless done so pursuant to a written court order or other lawful authorization requesting such action and with the affirmative intervention of MetroPCS' Staff VP Audit & Security Services or his designates. All written requests (i.e., court orders and subpoenas) from law enforcement agencies must be forwarded to the Compliance Department for review, approval, and implementation.

Interceptions of communications and access to call-identifying information shall only be made by MetroPCS Personnel authorized by MetroPCS' Staff VP Audit & Security Services and pursuant to appropriate authorization. A background check and a nondisclosure agreement shall be required for all authorized personnel. It is against Company policy for unauthorized personnel to intercept and/or access call-identifying information.

4.1 Exigent Circumstances

In certain limited situations, law enforcement personnel can declare that "Exigent Circumstances" exist that require, without a Subpoena or Court Order, respectively, (1) that certain customer information be turned over to them, (2) that a specific customer's service be turned off or on, or (3) that a Temporary PIN Register or Wiretap be granted for up to 48 hours. It is the responsibility of the Staff VP Audit & Security Services to determine the validity and authority for the declaration of Exigent Circumstances.

4.2 Responsibility For Oversight Of Process

The Staff VP Audit & Security Services shall oversee, review, and approve (refer to Section 3.3) all requests and shall ensure that each request is supported by appropriate legal authorization, as defined in Section 3.1. This responsibility requires expertise to recognize requests that meet federal and state statutes permitting interceptions. Responses to authorized and approved requests will be made in a timely manner with consideration given to the number of requests (i.e., workload) and the number of available personnel. Verbal requests for interceptions from law enforcement agencies shall not be honored unless Exigent Circumstances exist.

4.3 Records Retention

The Staff VP Audit & Security Services shall be responsible for maintaining secure and accurate records as required by the FCC's rules, including, but not limited to, the records of each interception (made with or without appropriate authorization). The Audit & Security Services Department will retain the original written request for record keeping purposes for a minimum of five years, and will record and store a certification that includes the following information for a minimum of five years:

- Telephone number(s) and/or circuit identification numbers
- Start date and start time of the interception and/or access to call identifying information
- Identity of the law enforcement officer presenting the authorization
- Name of the judge, magistrate, or prosecuting attorney signing the authorization
- Type of interception and/or access to call identifying information
- The name of the MetroPCS Personnel responsible for initiating the interception in accordance with the policies established herein.

This certification must be signed by the Staff VP Audit & Security Services or his designate. By his or her signature, such individual will 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 completion of the interception of the communications or access to call-identifying information.

4.4 Violations of Policy

MetroPCS will report any act of compromise of a lawful interception of communications or access to call-identifying information by unauthorized persons or entities, and any act of unlawful electronic surveillance that occurs on its premises, to the affected law enforcement agency or agencies within a reasonable time upon discovery. Violations of this Policy will also result in disciplinary action up to, and including termination of employment.

5.0 RESPONSIBILITY FOR COMPLIANCE

The Vice President & Chief Financial Officer shall be responsible for communicating this Policy to all MetroPCS personnel. The Staff VP Audit & Security Services and the authorized designates shall be responsible for ensuring compliance with the specific requirements as outlined in this Policy. The Staff VP Audit & Security Services will serve as the primary point of contact for law enforcement agencies and for all written requests. The Staff VP Audit & Security Services and the authorized designates shall be responsible for determining the appropriateness of all requests from law enforcement agencies.

The unauthorized interception of communications may have serious legal consequences for MetroPCS. Failure to meet the requirements of this Policy can result in disciplinary action up to and including termination and possible criminal prosecution. Employees who need assistance with understanding the requirements of this Policy should contact the Audit & Security Services Department. In addition, any violation of or departure from the policies set forth herein shall be reported immediately to the Staff VP Audit & Security Services.

metroPCS inc.

CALEA Procedures

Introduction

This document contains MetroPCS CALEA Procedures. These procedures are intended to implement the policy of MetroPCS as it relates to complying with Section 105 of the Communication Assistance for Law Enforcement Act ("CALEA").

1.0 PROCEDURES FOR HANDLING LAW ENFORCEMENT REQUESTS

When Law Enforcement Agencies contact MetroPCS personnel in the regional offices, retail stores or switch locations seeking assistance, the following procedures should be followed.

1.1 Normal Business Hours

During normal business hours (8:00 am - 6:00 pm CST - Monday thru Friday)

All requests for assistance from Law Enforcement Agencies made to any MetroPCS location during normal office hours should be referred to the Audit & Security Services Department in the Dallas office using the contact information in Exhibit A. It is the policy of MetroPCS that no work should be done concerning any law enforcement request without first obtaining the approval of the Staff VP Audit & Security Services or the authorized designate.

1.2 After Hours

After hours (5:00pm - 8:00am CST - Monday thru Friday, or Saturday and Sunday)

If Law Enforcement personnel contact MetroPCS Switch personnel during non-business hours, the person who speaks with the Law Enforcement Officer should obtain the following information and call the On-Call employee in the Audit & Security Services Department using the contact information in Exhibit A:

Name of Agent/Officer
- Agency/Department
- Contact Number
- Nature of the Emergency

Switch personnel should advise Law Enforcement that someone from the Audit & Security Services Department will contact them soon. The On-Call employee will verify the information with Law Enforcement, assess the situation, and determine if the situation is truly an emergency. After speaking with Law Enforcement, the On-Call employee will call the Switch to advise the appropriate person if anything needs to be done. In a true emergency, the On-Call employee from the Audit & Security Services Department may direct Switch personnel to perform the specified request made by Law Enforcement.

1.3 Exigent Circumstances

In certain limited situations, Law Enforcement personnel can declare that **"Exigent Circumstances"** exist that require that they be given access to customer information without a Subpoena or Court Order. Examples of Exigent Circumstances include kidnappings, hostage situations, and other life threatening emergencies where the delay in obtaining the normal Subpoena or Court Order could result in death or serious injury. When this occurs, Law Enforcement Agencies can request that MetroPCS turn off a customer's phone service or request a Temporary PIN Register or Wiretap lasting up to 48 hours, without a Subpoena or Court Order. If MetroPCS field personnel receive an **Exigent Circumstances** request, they should immediately notify the Audit & Security Services Department to seek guidance before taking any action.

At a minimum, requests for interceptions citing Exigent Circumstances must include:

a. the information, facilities, or technical assistance required.
b. the period of time during which the provision of information, facilities, or technical assistance is authorized.
c. a statement that no warrant or court order is required by law.
d. a statement that all statutory requirements have been met.
e. a statement that the specific requested assistance is required.
f. the signature of **EITHER** (i) the Attorney General of the United States, **OR** (ii) a law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

2.0 PROCESSING COURT ORDERS

Court Orders can only be processed by a MetroPCS employee or contractor authorized by the MetroPCS Staff VP Audit & Security Services and in accordance with the requirements of the MetroPCS CALEA Compliance Manual and the law.

Any Court Order served on MetroPCS by a Law Enforcement Agency or other authorized representative of a State or Federal Court, for the purpose of intercepting voice communications or other electronically transmitted customer data, (i.e., dialed digits, pages, short test messaging, wireless email, etc.) should be sent immediately to the Audit & Security Department to be processed as follows:

2.1 Validation

The Court Order should be checked to ensure that it includes the following information:

a. The Court Order must be directed to the correct corporate name.
b. The Court Order must specifically state what it is directing MetroPCS to do and the location of the facilities for which authority to intercept is granted.
c. Correct date.
d. Specifically states the length of time the intercept is to be carried out, (i.e., 30 days, 60 days, etc.). The Court Order cannot be open ended.
e. Judge's signature.
f. Court Order identifying a target that is, or has been a MetroPCS customer.
g. Verify that interception being requested is feasible and can be implemented with MetroPCS' existing technology.
h. The court order should be rejected and the appropriate law enforcement personnel should be notified immediately if the court order is deemed invalid for any reason. No additional action should be taken until a new court order is provided that is deemed valid.

2.2 LERMS

Assign the Court Order a case/reference number and enter appropriate information into log. At a minimum, the log must contain the following information. (See Exhibit B for example of Court Order Log.)

a. Telephone number(s) and/or circuit identification numbers.
b. Date Court Order was received.
c. Identity of the law enforcement officer presenting the authorization.

2.3 Prepare folder

At a minimum, the folder must contain the following information:

a. Court Order.
b. Case number.
c. Target number(s) and Circuit Number or T1 channel.
d. (MTA) or other MetroPCS location or region identifier.
e. Agency making the request.
f. Agent's name making request.
g. Type of request being made.
h. Date the Court Order was signed.
i. Date the Court Order was implemented.
j. Date the Court Order expires.
k. Any special directions or instruction for handling, (i.e., National Security Clearance, etc.)

2.4 Five Days Prior to Expiration Date

a. Contact issuing agent to determine whether Court Order is going to be extended.
b. If the order is extended, update log to reflect new Court Order termination date and include Court Order extension form in folder.
c. If not, ensure Court Order is promptly taken down on termination date.

2.5 Update log

a. Date and Time Court Order was removed.
b. Name of the MetroPCS employee responsible for taking down the Court Order.

2.6 File Court Order folder in a secure/locked location

2.7 Maintain approximately 6 months records on site for court appearances

3.0 PROCESSING SUBPOENAS

Subpoenas can only be processed by a MetroPCS employee or contractor authorized by the MetroPCS Staff VP Audit & Security Services and in accordance with the requirements of the MetroPCS CALEA Compliance Manual and the law.

Any subpoenas served on MetroPCS by a Law Enforcement Agency or authorized representative of a court of record for the purpose of receiving customer records should be sent to the Audit & Security Services Department to be processed as follows:

3.1 Validation

The subpoena should be checked to ensure that it includes the following information:

a. Correct corporate name.
b. Correct date.
c. Judge's signature.
d. Subpoena identifies a target or individual that is or has been a MetroPCS customer.
e. Information being requested is obtainable and can be provided to LEA.
f. The subpoena should be rejected and the appropriate Law Enforcement or court personnel should be notified immediately if the subpoena is deemed invalid for any reason. No additional action should be taken until a new subpoena is provided that is deemed valid.

3.2 Log

Assign the subpoena a case/reference number and enter appropriate information into log. At a minimum, the log must contain the following information. (See Exhibit B for example of Subpoena Log.)

a. Telephone number(s) and/or circuit identification numbers
b. Date subpoena was received
c. Identity of the law enforcement officer presenting the authorization
d. Case number
e. Customer name

3.3 Gather information requested

3.4 Send information to requesting agency

3.5 Prepare folder

At a minimum, the folder must contain the following information.

a. Subpoena.
b. Case number.
c. (MTA) or other MetroPCS location or region identifier.
d. Agency making the request.
e. Agent's name making request.
f. Type of request being made.
g. Copy of the requested information supplied to law enforcement agency.
h. Proof that requested information was delivered, (i.e., US Mail, Facsimile, UPS, FEDEX, email, etc.) If available, copy of the receipt for delivery (i.e., overnight delivery, courier, printed email conformation, etc.).

3.6 Update log

a. With date records were sent.

3.7 File subpoena/folder in a secure/locked location

3.8 Maintain approximately 6 months records on site for court appearances

4.0 UNAUTHORIZED SURVEILLANCE/COMPROMISE IN SURVEILLANCE

The following procedures should be followed in the event of an act of unauthorized surveillance or a compromise of previously authorized surveillance:

If any MetroPCS employee or contractor becomes aware of any act of unauthorized electronic surveillance or any compromise of authorized surveillance to unauthorized persons or entities, that employee or contractor shall report the incident immediately to the Staff VP Audit & Security Services.

The MetroPCS employee or contractor and the Staff VP Audit & Security Services shall promptly determine which law enforcement agencies are affected and notify such agencies of the incident.

The Staff VP Audit & Security Services shall compile a certification record for any unauthorized surveillance and ensure that all records available to MetroPCS regarding the surveillance (including any records of the contents of the interception) are placed in the appropriate file.

EXHIBIT A: Contact Information

General Contact Information for MetroPCS CALEA Issues

It is MetroPCS policy that interceptions of communications (i.e. wiretaps) using MetroPCS equipment or systems will only be activated pursuant to a written court order or other lawful authorization requesting such action.

All written requests (i.e. court orders, subpoenas and requests declaring Exigent Circumstances) from law enforcement agencies must be forwarded to the contact below for review, approval and implementation.

> **Note**: MetroPCS company policy prohibits the interception of customer communications and the provision of customer records to anyone without the prior authorization of the Staff VP Audit & Security Services or authorized designates.

The person named below, or his or her designate, is responsible for ensuring that any interception of communications or access to call identifying information requested by a law enforcement agency shall be activated only in accordance with a court order or other lawful authorization, and only in a manner consistent with MetroPCS' policies and procedures for CALEA compliance.

Mr. Steve Cochran
Staff VP Audit & Security Services
MetroPCS, Inc.
8144 Walnut Hill Lane Suite 800
Dallas, Texas 75231
1-800-571-1265 (daytime phone)
972-860-2635 (fax)
1-800-571-1265 (emergency after hours phone for On-Call employee)

The Staff VP Audit & Security Services may be reached during normal business hours at the daytime telephone number listed above. After hours requests will be taken by an On-Call employee. If the Staff VP Audit & Security Services is unavailable for any reason, he will designate another individual who also can be reached at the above business telephone number.

DATED: April 22, 2002
Revised : May 20, 2003
Revised: October 3, 2006