

7852 Walker Drive, Suite 200, Greenbelt, MD 20770
phone: 301-459-7590, fax: 301-577-5575
internet: www.jsitel.com, e-mail: jsi@jsitel.com

January 16, 2007

By Hand Delivery

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
c/o Natek, Inc., Inc.
236 Massachusetts Avenue, N.E. Suite 110
Washington, DC 20002

FILED/ACCEPTED
JAN 17 2007
Federal Communications Commission
Office of the Secretary

Re: ET Docket No. 04-295

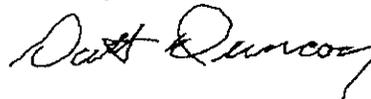
**Communications Assistance for Law Enforcement Act and Broadband
Access and Services**

**Amended Revised CALEA Section 105 SSI Policies and Procedures for
Sandhill Telephone Cooperative, Inc. 499 Filer ID No. 807816**

Dear Ms. Dortch:

On behalf of the telecommunications carrier listed above, John Staurulakis (JSI), its consultant is filing the attached amended revised CALEA Section 105 SSI Policies and Procedures together with four copies. The amendments are for the purpose of removing "confidential" from the document. Sandhill is not requesting confidential treatment. Please direct any questions regarding the filing to Scott Duncan or John Kuykendall at JSI or to Mr. Marshall Sowell, Sandhill Telephone Cooperative, Inc. CALEA Compliance Director. Mr. Sowell's contact information is included at Attachment A of the Policies and Procedures.

Sincerely,



Scott Duncan
JSI Staff Director-Regulatory Affairs
sduncan@jsitel.com

Attachment

Copies: 4 additional copies to Secretary

cc: David Ward, Senior Legal Advisor
Policy Division, Public Safety and Homeland Security Bureau
Marshall Sowell, Sandhill Telephone Cooperative, Inc.

No. of Copies rec'd 0+4
List ABOVE

Echelon Building II, Suite 200
9430 Research Boulevard, Austin, TX 78759
phone: 512-338-0473, fax: 512-346-0822

Eagandale Corporate Center, Suite 310
1380 Corporate Center Curve, Eagan, MN 55121
phone: 651-452-2660, fax: 651-452-1909

Brookside Court, Suite 135
4625 Alexander Drive, Alpharetta, GA 30022
phone: 770-569-2105, fax: 770-410-1608

547 South Oakview Lane
Bountiful, UT 84010
phone: 801-294-4576, fax: 801-294-5124

January 12, 2007

**CALEA SECTION 105
SYSTEM SECURITY AND INTEGRITY ("SSI")
POLICIES AND PROCEDURES MANUAL**

for

SANDHILL TELEPHONE COOPERATIVE, INC.

499 FILER ID 807816

122 South Main Street, P.O. Box 519
Jefferson, South Carolina 29718-0519
(843) 658-3434, (843) 658-7700 FAX

FILED/ACCEPTED
JAN 17 2007
Federal Communications Commission
Office of the Secretary

Notice: These revised Policies and Procedures replace in their entirety the Policies and Procedures filed previously by Sandhill Telephone Cooperative, Inc.

I. EFFECTIVE DATE

These policies and procedures have been adopted by SANDHILL TELEPHONE COOPERATIVE, INC. ("the Company") on **January 12, 2007** and shall remain in effect until notice is provided to the Federal Communications Commission ("FCC") regarding significant change or modification made pursuant to 47 C.F.R. § 1.20005(a).

For changes in the Company's CALEA Compliance Director or contact information, the Company will file with the FCC replacement attachments A and or B as circumstances indicate under the timeframe prescribed in 47 C.F.R. § 1.20005(a).

The definitions provided at Section III following apply to the entire document comprising the Company's Section 105 SSI policies and procedures.

II. STATEMENT OF POLICY

A. The following telecommunications services provided by the Company are subject to the Communications Assistance for Law Enforcement Act, Public Law No. 103-414, 10g Stat. 4279 (1994), ("CALEA"), and with the implementing regulations adopted by the Federal Communications Commission ("FCC") codified at Part 1, Subpart Z of the FCC's rules, 47 C.F.R. §§ 1.20000 through 20007.

Incumbent Local Exchange Carrier ("ILEC") wireline circuit-switched telecommunications services.

ILEC circuit-switched packet-mode communications.

Facilities-based broadband Internet access services.

B. It is the policy of the Company to comply with CALEA, FCC rules respecting CALEA and Federal Bureau of Investigation ("FBI") requirements respecting CALEA. In particular, it is the policy of the Company that each and every call content interception, call information interception or other electronic surveillance measure effected within its switching premises or facilities-based broadband Internet access router premises must be implemented and activated in accordance with appropriate legal authorization, with appropriate Company authorization, and with the affirmative intervention of one of the Company's officers or employees acting in accordance with FCC regulations.

C. The Company has appointed the CALEA Compliance Director identified in Attachment A and senior officers and employees identified in Attachment B as its Primary and Secondary Points of Contact with law enforcement for CALEA purposes. These are the only officers and employees of the Company authorized to implement and activate call content interceptions (wiretaps), call information interceptions (pen registers, and traps and traces) and other electronic surveillance measures. These individuals shall be familiar with the policies and procedures set forth herein.

D. The Company will facilitate authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects - (1) privacy and security of communications and call-identifying information not authorized to be intercepted; and (2) against information regarding the government's interception of communications and access to call-identifying information being disclosed to customers, Company employees not involved in assisting law enforcement with the interception or law enforcement personnel not identified by the court order for the intercept.

E. Any employee of the Company who has not been designated as the CALEA Compliance Director or a Primary or Secondary Point of Contact shall refer any requests for call content interceptions (wiretaps), call information interceptions (pen registers, and traps and traces) and other electronic surveillance measures to one of the individuals designated at Exhibit B as a Primary or Secondary Point of Contact.

F. Any employee who becomes aware of surveillance performed by an employee or any other party without appropriate legal authorization shall report the surveillance to the Company's CALEA Compliance Director immediately.

G. The Company CALEA Compliance Director will 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 occurs on the Company's premises.

H. Any employee who knowingly uses the Company's capabilities for call content interception or call information interception or other means of electronic surveillance in violation of these policies and procedures will face severe disciplinary action up to and including termination of employment.

III. DEFINITIONS

As used in these CALEA Policies and Procedures, the following terms shall have the meaning defined in this Section III.

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.

Appropriate carrier authorization. The term “appropriate carrier authorization” means the policies and procedures adopted by the Company to supervise and control officers and employees authorized to assist law enforcement in conducting any interception of communications or access to call-identifying information or other forms of electronic surveillance.

Appropriate authorization. The term “appropriate authorization” means both appropriate legal authorization and appropriate carrier authorization.

CALEA. Communications Assistance for Law Enforcement Act, Public Law No. 103-414, 108 Stat. 4279 (1994). CALEA is codified at (codified as amended in sections of 18 U.S.C. and 47 U.S.C.).

Call content interception. The term “Call content interception” means an interception of a communication, including its content (e.g., a wiretap carried out pursuant to a court order issued in accordance with Title III).

Call identifying information (“CII”). The term “call-identifying information” means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier. Law enforcement agencies (LEAs) generally access CII by use of pen registers and trap-and-trace devices.

Call information interception. The term “call information interception” means accessing dialing or signaling information that identifies the origin, direction, destination, or termination of a communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier (e.g., a pen register or trap-and-trace surveillance).

Carrier. For purposes of these CALEA Policies and Procedures, “carrier” as used in any definition or other context shall be SANDHILL TELEPHONE COOPERATIVE, INC. (“Company”).

Company. SANDHILL TELEPHONE COOPERATIVE, INC..

Contents. “Contents” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.

Destination. A party or place to which a call is being made (e.g., the called party).

Electronic surveillance. “Electronic surveillance” with respect to communications that are carried by circuit-switched facilities and switched by a circuit-switch or carried by facilities-based broadband Internet access service includes but is not limited to (a) the interception of call content (b) access to CII (c) acquisition of location-related information concerning a service subscriber or facility, (d) preservation of any of the above information or (e) access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above.

Facilities-Based Broadband Internet Access Service. Facilities-based broadband Internet access service is transmission or switching over the Company’s facilities between the end user and the Internet Service Provider (ISP). Electronic communications over facilities-based broadband Internet access are fully subject to these policies and procedures.

Federal Wiretap and Surveillance Statutes. Federal statutes governing electronic surveillance, including but not limited to requirements for legal authorization for federal LEAs to conduct electronic surveillance, include but are not limited to the following:

Title III of the 1968 Federal Wiretap Act

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Codified at Title 18, Crimes and Criminal Procedures, Part I, Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications (18 U.S.C. §§ 2510-2522). In order for a wiretap to be put in place, the Federal Wiretap Act generally requires a court order issued by a judge who must conclude, based on an affidavit submitted by the government, that there is probable cause to believe that a crime has been, is being, or is about to be committed.

Pen Register and Trap and Trace Statute or Pen/Trap Statute

Title III of the Electronic Communications and Privacy Act of 1986 (ECPA). Codified at Title 18, Crimes and Criminal Procedures, Part II, Criminal Procedure, Chapter 206, Pen Registers and Trap and Trace Devices, 18 U.S.C. §§ 3121-3127.

Foreign Intelligence Surveillance Act of 1978 (FISA)

Title 50, War and National Defense, Chapter 36, Foreign Intelligence Surveillance, 50 U.S.C. §§ 1801-1811 (Foreign Intelligence Surveillance Act).

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56), commonly known as the USA PATRIOT Act or simply the Patriot Act.

Congress passed the Patriot Act after the September 11, 2001 attacks as a response to the threat of terrorist attacks against the United States. The Patriot Act dramatically expanded the authority of LEAs for the purpose of combating terrorism. Congress renewed the Patriot Act on March 2, 2006. Among the powers granted LEAs to combat terrorism were amendments to the Title 18 wiretap and pen register/trap and trace laws together with the Title 50 foreign intelligence surveillance provisions.

Government. The term "government" means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.

Intercept. "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

Interconnected-VoIP. Interconnected VoIP services include those VoIP services that: (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require Internet Protocol-compatible customer premises equipment; and (4) permit users to receive calls from and terminate calls to the public switched telephone network. Interconnected-VoIP is fully subject to CALEA and these policies and procedures.

Law Enforcement Agency (LEA). The term "law enforcement agency" or "LEA" means authorized government law enforcement agency or a U.S. intelligence agency.

Origin. A party initiating a call (e.g., a calling party), or a place from which a call is initiated.

Pen Register. The term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

State Surveillance Statutes: State laws applicable to electronic surveillance include, but are not limited to, Sections 17-29-10 through 17-29-50.

Subject-Initiated Dialing and Signaling Information. "Subject-Initiated Dialing and Signaling Information" is capability that permits a LEA to be informed when a subject using the facilities under surveillance uses services that provide call identifying information, such as call forwarding, call waiting, call hold, and three-way calling. Excludes signals generated by customer premises equipment when no network signal is generated.

Termination. A party or place at the end of a communication path (e.g. the called or call receiving party, or the switch of a party that has placed another party on hold).

Trap and Trace. The term "trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

VoIP. Voice over Internet Protocol (VoIP) includes any IP-enabled services offering real-time, multidirectional voice functionality, including, but not limited to, services that mimic traditional telephony.

IV. COMPANY CALEA COMPLIANCE DIRECTOR

The Company has appointed a senior officer or employee responsible for ensuring that any electronic surveillance, including but not limited to interception of communications or access to call-identifying information, effected within the Company's 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.

The Company CALEA Compliance Director is indicated at Attachment A. The Company CALEA Compliance Director may also serve as a Primary Point of Contact or Secondary Point of Contact. If such is the case, the individual will be indicated on both Attachment A and Attachment B.

V. CALEA PRIMARY AND SECONDARY POINTS OF CONTACT

A. Primary Point of Contact

The Company's Primary Point of Contact ("PPOC") is a senior officer or employee appointed by the Company 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. The PPOC's duties include, but are not limited to, the duties listed in Section V.C below. The Company's PPOC and contact information are listed on Attachment B.

B. Secondary Point of Contact

The Company's Secondary Point(s) of Contact ("SPOC" or "SPOCs") are the point(s) of contact for law enforcement officials and agencies regarding CALEA-related matters when the PPOC is unavailable. Their duties include, but are not limited to, the duties listed in Section V.C below (excluding those duties indicated as limited to the PPOC, unless otherwise delegated to the SPOC by the PPOC). The Company's SPOCs and related contact information are listed on Attachment B.

C. PPOC and SPOC Duties:

The PPOC and SPOC duties include but are not limited to, the following (unless otherwise indicated, the duties may be executed by either the PPOC or the SPOC).

1. Responding to questions and inquiries from law enforcement officials and agencies regarding call content interceptions (e.g., wiretaps), call information interceptions (e.g., pen registers or traps and traces surveillance) and other electronic surveillance activities.
2. Reviewing the orders, warrants, or other authorizations presented by law enforcement officials requesting call content interceptions, call information interceptions and other electronic surveillance and making a reasonable determination that:
 - such documents are what they purport to be; and
 - such documents constitute **appropriate legal authorization** for the requested call content interception, call information interception or other electronic surveillance; and
 - determining whether the specifically requested measures can be implemented technically.
3. Implementing (or overseeing the implementation by a competent technical employee) of properly authorized (that is, those having both **appropriate legal authorization** and **appropriate carrier authorization**) call content interceptions, call information interceptions and other electronic surveillance.
4. Becoming and remaining aware of additional relevant federal and state statutory provisions regarding the authorization (including those involving exigent circumstances) of call content interceptions, call information interceptions and other electronic surveillance measures.
5. Reporting the following to the affected law enforcement agencies within a reasonable time upon discovery: (a) any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities; and (b) any act of unlawful electronic surveillance that occurred on its premises.
6. Preparing and signing a complete and accurate certification for each and every call content interception, call information interception and other electronic surveillance measure implemented by the Company. A certification form is attached hereto as Attachment C. Such certification contains the elements described in Section VI below.
7. With respect to the PPOC, supervising the maintenance of records pursuant to the requirements of Section VI below.
8. With respect to the PPOC, supervising, as needed, performance by the SPOC of any CALEA related duties.

VI. MAINTENANCE OF RECORDS

The Company will maintain a secure and accurate record of each call content interception, call information interception and other electronic surveillance measure implemented by the Company, made with or without appropriate authorization, in the form of single certification. A certification for use in this regard is attached hereto as Attachment C.

A. Certification Content

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 person signing the appropriate legal authorization.
5. The type of interception of communications or access to call-identifying information (*e.g.*, pen register, trap and trace, Title III, FISA).
6. The name of the PPOC or SPOC overseeing implementation of the call content interception, call information interception or other electronic surveillance measure and who is acting in accordance with the Company's CALEA policies and procedures described herein.
7. The signature of the PPOC or SPOC preparing the certification. The PPOC or SPOC, by his/her signature, will certify that the record is complete and accurate.

B. Certification Timeframe

This certification must be compiled either contemporaneously with, or within a reasonable period of time after the initiation of the call content interception, call information interception or other electronic surveillance measure implemented by the Company.

C. Maintenance of Records

The Company shall maintain the certificates described in Section VI.A. for a period of ten years following the date of termination or completion of the call content interception, call information interception or other electronic surveillance measure.

January 12, 2007

Attachment A

SANDHILL TELEPHONE COOPERATIVE, INC.

499 FILER ID 807816

122 South Main Street, P.O. Box 519
Jefferson, South Carolina 29718-0519
(843) 658-3434, (843) 658-7700 FAX

COMPANY CALEA COMPLIANCE DIRECTOR

Name: Marshall Sowell
Title: Operations Manager
Telephone Number: (843) 658-3111
Alternate Number: (843) 672-8240
E-mail: mlsowell@shtc.net

Date Appointed: January 12, 2007

Attachment B

For

SANDHILL TELEPHONE COOPERATIVE, INC.

499 FILER ID 807816

122 South Main Street, P.O. Box 519
Jefferson, South Carolina 29718-0519
(843) 658-3434, (843) 658-7700 FAX

**CALEA Primary and Secondary Points of Contact –
for both Circuit-Switched Communications and Broadband**

Primary Point of Contact (PPOC)

Name: Dean Gulledge
Title: Network Engineer
Telephone Number: (843) 658-6840
FAX: (843) 658-7700
E-mail: dgulledge@shtc.net
Outside of business hours, on a seven days a week, 24 hours a day basis,
the PPOC can be reached by:
Home Telephone Number: (843) 623-3326
Cell Phone Number: (843) 672-8169

Secondary Point(s) of Contact (SPOC)

Name: Howard Smith
Title: IT Technician
Telephone Number: (843) 658-3393
FAX: (843) 658-7700
E-mail: howardsmith@shtc.net
Outside of business hours, on a seven days a week, 24 hours a day basis,
the SPOC can be reached by:
Home Telephone Number: (843) 675-5300
Cell Phone Number: (843) 622-5907

Attachment C

SANDHILL TELEPHONE COOPERATIVE, INC. ELECTRONIC SURVEILLANCE CERTIFICATION

I, _____ [name], hereby certify that I have been duly authorized to serve as the Primary or Secondary Point of Contact of **SANDHILL TELEPHONE COOPERATIVE, INC.**, and in that position, have assisted law enforcement in the implementation and activation of the identified interception of communications or access to call-identifying information:

1. Identity of Law Enforcement Officer(s)
Presenting the Appropriate Legal Authorization: _____
2. Name of Person Signing the
Appropriate Legal Authorization: _____
3. Type of Interception or Access
(Title III wiretap, pen register,
trap and trace, FISA surveillance): _____
4. Telephone number(s) and/or circuit
identification numbers involved: _____
5. Start date: _____
6. Time of the opening of the
circuit for law enforcement: _____
7. Officer or employee responsible
For oversight and compliance with
Company policies and FCC rules: _____

I have attached photocopies and/or notes regarding the court order or other legal authorization (including any extensions), the identification of the law enforcement officer presenting the authorization, and any exigent circumstances.

By my signature, I certify that I have overseen the interception of communications or access to call-identifying information described above, and that this Certification is complete and accurate.

Signed: _____

Date: _____