CALEA

SYSTEM SECURITY AND INTEGRITY POLICIES AND PROCEDURES

ADOPTED BY THE EL RENO MUNICIPAL AUTHORITY BOARD OF DIRECTORS

September 12, 2023

EL RENO MUNICIPAL AUTHORITY/CITY OF EL RENO

101 NORTH CHOCTAW AVENUE
PO DRAWER 700
EL RENO, OK 73036

(Main Phone) 405-262-4070

(Fax) 405-_____

_____@elrenook.gov

TABLE OF CONTENTS

STATEMENT OF POLICY

It is the policy of the El Reno Municipal Authority, a municipal trust of the City of El Reno, Oklahoma, being hereafter jointly referred to as ("Carrier") to comply with the Communications Assistance for Law Enforcement Act, Public Law No. I 03- 414, 108 Stat. 4279 (1994), ("CALEA"), with the Federal Communications Commission ("FCC") and Federal Bureau of Investigation ("FBI") regulations implementing the statute. These obligations include 47 C.F.R, Part 1, Subpart Z, §1.20000-1.20008 [as consolidated in the FCC's Second Report and Order, ET Docket No. 04-295, Released May 12, 2006, Fed. Reg. 38091, et seq., July 5, 2006], Title III of The Omnibus Crime Control and Safe Streets Act of 1968 [18U.S.C. §§ 2510-2520], The Electronic Communications Privacy Act of 1986 [18 U.S.C. §§ 2701- 2712, §§ 3121-3127] and The Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. §§ 1801- 1829, 1841-1861][as amended by the USA PATRIOT Act of 2001, and The PATRIOT Reauthorization Act of 2006], and the applicable state wiretapping laws.

In particular, it is the policy of Carrier to ensure that any interception of communications or access to call-identifying information effected within its facilities can be activated only in accordance with appropriate legal authorization, with appropriate Carrier authorization, and with the affirmative intervention of an individual officer or employee of Carrier acting in accordance with regulations prescribed by the FCC. All officers, employees, or agents are required to follow the policies and procedures specified in this compliance manual.

Carrier has appointed the senior officers and employees identified in Exhibit A as its Primary and Secondary Points of Contact with law enforcement agencies and officials for CALEA purposes. These are the only officers and employees of Carrier who are authorized to implement and activate interceptions of communications (wiretaps) or access to call-identifying information (pen registers, and traps and traces), and who are responsible for affirmatively intervening to ensure that such interceptions or access can be activated only in accordance with appropriate legal authorization. Also, an agent or Trusted Third Party ("TTP") may be appointed by the Carrier to implement, with the approval of the senior officer or employee, the Technical Assistance order by a court and to be available twenty-four hours a day, seven days a week, for the Law Enforcement Agency ("LEA"). All of these senior officers, employees, agents or TTPs of Carrier are familiar with the policy set forth above, and with the implementing procedures set forth on the following pages, exhibits and appendices.

IMPLEMENTING PROCEDURES

1.0 Primary and Secondary Points of Contact for Law Enforcement.

1.1 Appointment of Primary Point of Contact. Carrier has appointed the senior officer or employee identified on Exhibit A as its CALEA Compliance Manager, to serve as the Primary Point of Contact with law enforcement agencies and officials for CALEA purposes. This employee of Carrier is responsible for affirmatively intervening to ensure that interceptions of communications (wiretaps) or access to call-identifying information (pen registers, and traps and traces) are activated only in accordance with appropriate legal authorization.

1.2 Appointment of Secondary Points of Contact. In the event that law enforcement agencies and officials are unable to reach Carrier's CALEA Compliance Manager, Carrier has appointed the senior officers and employees listed on Exhibit A as its Assistant CALEA Compliance Managers, to serve as the Secondary Points of Contact with law enforcement agencies and officials for CALEA purposes. If Carrier's Primary Point of Contact is unavailable, one or more of these senior officers or employees of Carrier is responsible for affirmatively intervening to ensure that interceptions of communications (wiretaps) or access to call identifying information (pen registers, and traps and traces) are activated only in accordance with appropriate legal authorization.

1.3 Appointment Forms. The Carrier's General Manager will appoint its CALEA Compliance Manager and as many Assistant CALEA Compliance Managers as they deem necessary, and will execute an Appointment Form of the type attached as Exhibit B for each individual. These Appointment Forms will serve as express written documentation that the Carrier has given these

senior officers and employees the required "Appropriate Carrier Authorization" to assist law enforcement in conducting any interception of communications or access to call- identifying information. Appointments remain in effect until they are terminated by the General Manager. The date of such termination will be expressly noted on the Appointment Form.

2.0 Law Enforcement Access to Primary and Secondary Points of Contact.

2.1 Designation of “On Duty” Point of Contact. Designation of “On Duty" Carrier's CALEA Manager is responsible for ensuring that a Primary or Secondary Point of Contact is available to law enforcement officials at all times-that is, on a seven days per week, twenty-four hours per day basis. Carrier's CALEA Compliance Manager will be "on duty" as the Primary Point of Contact as much as possible during both business and non-business hours, and will be responsible for leaving contact information with Carrier's receptionists, telephone answering service and/or voice mail system. In the event that Carrier's CALEA Compliance Manager will not be available to law enforcement officials, she is responsible for designating one or more of Carrier's Assistant CALEA Compliance Managers to serve as the "on duty" Point(s) of Contact during that period, and for making sure that the appropriate contact information is left with Carrier's receptionists, telephone answering service and/or voice mail system.

2.2 Business Hours. During Carrier's normal business hours, the employees greeting visitors at Carrier's main business office and the employees answering Carrier's main telephone number will be instructed and trained to refer all visits or inquiries by law enforcement officials regarding wiretaps, pen registers, traps and traces, and other electronic surveillance activities to the Carrier's CALEA Compliance Manager, or, in her absence, to the Assistant CALEA Compliance Manager designated as the "on duty" Point of Contact.

2.3 Non-Business Hours. At all times when the Carrier's main business office is closed, its telephone answering service or voice mail system will be directed or programmed to forward calls by law enforcement officials regarding wiretaps, pen registers, traps and traces, and other electronic surveillance activities to the Carrier's CALEA Compliance Manager, or, in her absence, to the Assistant CALEA Compliance Manager designated as the "on duty" Point of Contact.

3.0 Job Functions of Primary and Secondary Points of Contact.

3.1 Primary Point of Contact. Carrier's CALEA Compliance Manager is responsible for serving as Carrier's Primary Point of Contact with law enforcement officials and agencies regarding all CALEA-related matters. These duties include:

a. responding to questions and inquiries from law enforcement officials and agencies regarding wiretaps, pen registers, traps and traces, and other electronic surveillance activities;

b. reviewing the orders, warrants, or other authorizations proffered by law enforcement officials requesting implementation of wiretaps, pen registers, traps and traces, or other electronic surveillance measures to make a reasonable determination whether such documents are what they purport to be;

c. reviewing the orders, warrants, or other authorizations proffered by law enforcement officials requesting implementation of wiretaps, pen registers, traps and traces, or other electronic surveillance measures to determine whether the specifically requested measures can be implemented technically;

d. implementing (or overseeing the implementation by a competent technical employee) of properly authorized (that is, having both appropriate legal authorization and appropriate carrier authorization) wiretaps, pen registers, traps and traces, or other electronic surveillance measures;

e. becoming and remaining aware of additional relevant federal and state statutory provisions regarding the authorization (including those involving exigent circumstances) of wiretaps, pen registers, traps and traces, or other electronic surveillance measures, including the Omnibus Crime Control And Safe Streets Act of 1968 and the Electronic

Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-20, 2701-10 and 3121-26), the Foreign Intelligence Surveillance Act (50 U.S.C. §§ 1801-11), and collateral state electronic surveillance statutes;

f. reporting any and all acts of unauthorized or unlawful electronic surveillance occurring on Carrier's premises to the appropriate law enforcement agency within a reasonable time period (not to exceed five business days) after their discovery;

g. reporting any and all compromises of the security or integrity of lawful wiretaps, pen registers, traps and traces, or other electronic surveillance measures by unauthorized persons or entities to the appropriate law enforcement agency within a reasonable time period (not to exceed five business days) after their discovery;

h. preparing and signing a complete and accurate certification (or reviewing the certifications prepared by Assistant CALEA Compliance Managers) for each and every wiretap, pen register, trap and trace, or other electronic surveillance measure implemented by Carrier;

i. supervising the maintenance and retention of secure and accurate records of the wiretaps, pen registers, traps and traces, or other electronic surveillance measures implemented by Carrier for a period of ten years after the termination of the surveillance measure;

j. reviewing and revising, if necessary, the present CALEA Compliance Policies and Procedures after significant changes in federal or state electronic surveillance statutes, or relevant FCC rules;

k. training and supervising the activities of Assistant CALEA Compliance Managers;

l. designating the Assistant CALEA Compliance Manager(s) who are the Carrier's "on duty" Point(s) of Contact for law enforcement at times when the CALEA Compliance Manager is unavailable; and

m. ensuring that this manual is updated with the FCC within 90 days of any amendment or merger with another telecommunications carrier.

3.2 Secondary Points of Contact. Carrier's CALEA Assistant Compliance Managers are responsible for serving as its Secondary Point(s) of Contact with law enforcement officials and agencies regarding CALEA-related matters when the CALEA Compliance Manager is unavailable. Their duties include:

a. reviewing the orders, warrants, or other authorizations proffered by law enforcement officials requesting implementation of wiretaps, pen registers, traps and traces, or other electronic surveillance measures to make a reasonable determination whether such documents are what they purport to be;

b. reviewing the orders, warrants, or other authorizations proffered by law enforcement officials requesting implementation of wiretaps, pen registers, traps and traces, or other electronic surveillance measures to determine whether the specifically requested measures can be implemented technically;

c. implementing (or overseeing the implementation by a competent technical employee) of properly authorized (both appropriate legal authorization and appropriate carrier authorization) wiretaps, pen registers, traps and traces, or other electronic surveillance measures;

d. becoming and remaining aware of additional relevant federal and state statutory provisions regarding the authorization (including those involving exigent circumstances) of wiretaps, pen registers, traps and traces, or other electronic surveillance measures, including the Omnibus Crime Control And Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-20, 2701-10 and 3121-26), the Foreign Intelligence Surveillance Act (50 U.S.C. §§ 1801-11), and collateral state

electronic surveillance statutes;

e. reporting any and all unauthorized or unlawful electronic surveillance occurring on Carrier's premises to the CALEA Compliance Manager as soon as possible after discovery;

f. reporting any and all compromises of the security or integrity of lawful wiretaps, pen registers, traps and traces, or other electronic surveillance measures by unauthorized persons or entities to the CALEA Compliance Manager as soon as possible after discovery; and

g. preparing and signing a complete and accurate certification for each and every wiretap, pen register, trap and trace, or other electronic surveillance measure that he or she supervises or implements on behalf of Carrier.

4.0 Appropriate Authorization.

4.1 No interception of communications or access to call-identifying information may be implemented on Carrier's premises without both "appropriate carrier authorization" and "appropriate legal authorization." The term "appropriate carrier authorization" means that Carrier has formally appointed the officer or employee assisting law enforcement to be its CALEA Compliance Manager or one of its Assistant CALEA Compliance Managers, and has expressly authorized the officer or employee to receive and evaluate requests by law enforcement agencies and officials for interception of communications or access to call-identifying information, and to implement or supervise the implementation of such interceptions or access. The term "appropriate legal authorization" means that the law enforcement agency or official requesting an interception of communications or access to call-identifying information has obtained a signed court order, signed warrant or other valid authorization permitted by 18 U.S.C. §§ 2518(7) or any other relevant federal or state statute.

4.2 No officer or employee of Carrier can become the CALEA Compliance Manager or an Assistant CALEA Compliance Manager without being appointed to the position by the Carrier's General Manager, and without receiving and signing a completed Authorization Form (of the type attached as Exhibit B) executed by the Carrier's General Manager.

4.3 Only the CALEA Compliance Manager or an Assistant CALEA Compliance Manager designated by the CALEA Compliance Manager as an "on duty" Point of Contact with law enforcement is authorized by the Carrier to receive a request from any law enforcement agency or official for an interception of communications or access to call-identifying information, to examine and determine whether the requesting law enforcement agency or official has appropriate legal authorization, and to implement or supervise the implementation of an interception of communications or access to call identifying information.

4.4 No officer or employee of Carrier who has not been appointed its CALEA Compliance Manager or an Assistant CALEA Compliance Manager may accept or review a request from any law enforcement agency or official for an interception of communications or access to call-identifying information. All such requests (and accompanying court orders or other documents) must be referred immediately to the CALEA Compliance Manager or (if she is unavailable) to an Assistant CALEA Compliance Manager "on duty" at the time. No officer or employee of Carrier other than its CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager may physically implement or activate a wiretap, pen register, trap and trace, or other electronic surveillance measure unless he or she is subject at all times to the direct supervision and oversight of the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager.

4.5 The Carrier’s CALEA Compliance Manager or “on duty” Assistant CALEA Compliance Manager will not activate, or supervise the activation of, an interception of communications or access to call-identifying information unless and until presented by an identified law enforcement official possessing credentials which reasonably appear to be valid with either:

a. document which reasonably appears to be a valid court order authorizing the interception of wire or electronic communication, the installation and use of a pen register

or a trap and trace device, or authorizing electronic surveillance under the Foreign Intelligence Surveillance act; or

b. a document which reasonably appears to indicate that the identified official is a specially designated representative of the U.S. Attorney General, or (in cases not involving the Foreign Intelligence Surveillance Act) a Deputy Attorney General, Associate Attorney General or principal federal or state prosecuting attorney for the area, and a claim by such official that an emergency situation exists that requires the immediate initiation of an interception of communications or access to call-identifying information without a court order. In the event of such an asserted emergency, (i) an interception must be terminated if a court order is not sought within 48 hours or is denied; (ii) an access to call identifying information must be terminated if a court order is not obtained within 48 hours; and (iii) an electronic surveillance under the Foreign Intelligence Surveillance Act must be terminated if an order authorizing it is not obtained within 24 hours.

5.0 Reasonable Determination of Appropriate Legal Authorization.

5.1 Interception of Communications (wiretaps). In reviewing a court order authorizing or approving a wiretap to determine whether it is what it purports to be, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager should look to see whether it contains most or all of the following elements:

a. the signature of a judge of the federal or state court (U.S. Court of Appeals, U.S. District Court or state court having general criminal jurisdiction) for the circuit or district in which Carrier is located, or the circuit or district in which law enforcement will receive the intercepted communications;

b. the name(s) or description of the person whose communications are to be intercepted;

c. the address or geographic location, and landline or mobile telephone number(s), of the communications facilities to be intercepted;

d. a description of the type of communication sought to be intercepted;

e. a statement of the particular type(s) of criminal offense to which the communications relate;

f. the name of the federal or state law enforcement agency authorized to intercept the communications;

g. the name of the law enforcement official authorizing the application for the order;

h. the period of time (not greater than 30 days) during which interception is authorized;

i. a statement whether or not the interception will automatically terminate when the described communication is first intercepted and obtained;

j. a directive that the Carrier shall furnish the authorized law enforcement agency forthwith with all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that Carrier is according the person whose communications are to be intercepted;

k. a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception, and must terminate upon attainment of the authorized objective, or in any event in 30 days; and

l. a requirement that reports be made to the issuing judge showing what progress has been made toward achievement of the authorized objective, and the need for continued interception.

5.2 Access to Call-Identifying Information (pen registers, and traps and traces). In reviewing

a court order authorizing the installation and use of a pen register or trap and trace device to determine whether it is what it purports to be, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager should look to see whether it contains most or all of the following elements:

a. the signature of a judge or magistrate of the federal or state court (U.S. Court of Appeals, U.S. District Court or state court having general criminal jurisdiction) for the circuit or district in which Carrier is located, or the circuit or district in which law enforcement will receive the call-identifying information;

b. the identity of the person to whom is leased, or in whose name is listed, the telephone line to which the pen register or trap and trace device is to be attached;

c. the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached;

d. the geographic limits of the trap and trace order;

e. a statement of the criminal offense to which the information likely to be obtained by the pen register or trap and trace relates;

f. the name of the federal or state law enforcement agency authorized to use the call-identifying information;

g. the name of the law enforcement official authorizing the application for the order;

h. the period of time (not greater than 60 days) during which the pen register, or trap and trace, is authorized;

i. a directive that the Carrier shall furnish the authorized law enforcement agency with the information, facilities and technical assistance necessary to accomplish the installation of the pen register or trap and trace device;

j. a directive that the order be sealed until otherwise ordered by the court;

k. a directive that the Carrier not disclose the existence of the pen register or trap and trace device, or the existence of the investigation, to the listed subscriber, or to any other person, unless and until otherwise ordered by the court; and

l. a directive that the Carrier shall not disclose (i) the contents of any communication, (ii) the name, address, or financial information of a subscriber or customer, or (iii) cell site location or global positioning system information.

5.3 Foreign Intelligence Surveillance Act. In reviewing a court order authorizing or approving electronic surveillance under the Foreign Intelligence Surveillance Act to determine whether it is what it purports to be, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager should look to see whether it contains most or all of the following elements:

a. the identity, if known, or a description of the target of the electronic surveillance;

b. the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which a pen register or trap and trace device is to be attached or applied;

c. the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which a pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

d. the type of information sought to be acquired, and the type of communications or activities to be subjected to the surveillance;

e. a statement that the carrier shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the

court;

f. the period of time, not to exceed 90 days absent an extension that does not exceed 90 days, during which the electronic surveillance is approved; provided, however, that where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, may be for a period not to exceed one year;

g. the minimization procedures to be followed;

h. a directive that the Carrier shall furnish the authorized law enforcement agency forthwith all information, facilities, and technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that Carrier is providing the target of electronic surveillance;

i. a directive that the Carrier maintain under security procedures approved by the U.S. Attorney General and Director of Central Intelligence any records concerning the surveillance or aid furnished that the Carrier wishes to retain; and

j. a statement that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order):

(A) the name of the customer or subscriber;

(B) the address of the customer or subscriber;

(C) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and

(D) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;

(ii) in the case of a provider of local or long-distance telephone service, any local or long-distance telephone records of the customer or subscriber:

(A) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and

(B) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service;

5.4 Reasonable Determination of Validity. Where most or all of the foregoing elements are included in the particular type of court order proffered by the identified law enforcement official, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager may reasonably determine that the court order is what it purports to be, and proceed to affirmatively intervene and assist law enforcement in implementing and conducting the authorized interception of communications or access to call identifying information. The CALEA Compliance Manager or “On duty" Assistant CALEA Compliance Manager is not authorized to test the accuracy of the statements in a proffered court order, or otherwise to conduct his or her own independent or "de novo" review of the validity of such court order, prior to implementing the subject interception of communications or access to call-identifying information.

5.5 Future Statutory Changes. The foregoing listings of the elements of typical court orders are based upon the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic

Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-20, 2701-10 and 3121-26), and the Foreign Intelligence Surveillance Act (50 U.S.C. §§ 1801-11), as they existed on or prior to the date of this Manual. Future changes in these statutes, or their judicial interpretation, may modify the elements required to be included in court orders for various types of electronic surveillance.

5.6 State Statutes. State statutes may impose additional requirements and restrictions upon the obtaining of state court orders by state and local law enforcement officials for wiretaps, pen registers, traps and traces, and other electronic surveillance measures. The CALEA Compliance Manager will consult with Carrier's local counsel periodically to determine whether and how such state statutes (if any) will impact the nature and typical elements of state court orders which the CALEA Compliance Manager or “On duty” Assistant CALEA Compliance Manager may have to review.

6.0 Emergency Circumstances When No Court Order May Be Required.

6.1 Emergency Situations. In the event of an emergency situation, technical assistance for wiretaps, pen registers, traps and traces, and other electronic surveillance activity, the LEA should contact the Carrier's Compliance Manager using the contact information in Exhibit A. In these circumstances the Carrier requires a written statement from a supervisory representative of the LEA. Except in extraordinary circumstances, no technical assistance will be provided to the LEA without the LEA completing the Emergency Electronic Surveillance Request Form in Exhibit D. The Compliance Manager should email or fax this form to the LEA. While the LEA is completing the form, the Compliance Manager should proceed to make arrangements for the provision of technical assistance. Upon the receipt of a properly completed Exhibit D, technical assistance may be provided in accordance with applicable federal and state laws. This period should normally be no longer than 48 hours. Legal Counsel from the City Attorney’s Office should be sought to provide the Compliance Manager with the applicable time periods for which technical assistance under emergency circumstances may be allowed under law. Technical assistance will be terminated within the lawful time period, unless the LEA has obtained an appropriate court order, the information sought by the LEA was obtained, or the application for a court order was denied before the lawful time period had expired.

6.2 Interceptions of Communications (wiretaps). In very limited emergency situations, specially designated law enforcement officials may request and obtain the activation of a wiretap before getting a court order. The present criteria in 18 U.S.C. Sec. 2518(7) require that:

a. the requesting law enforcement official have received "special designation" (which should be documented) from the U.S. Attorney General, the Deputy U.S. Attorney General, the Associate U.S. Attorney General, or the principal prosecuting attorney of a State or State subdivision (county or city);

b. an emergency situation exists involving immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest, or an ongoing attack on a protected computer; and

c. an application for a court order must be made within 48 hours after the interception is initiated, and must be granted.

6.3 Access to Call-Identifying Information (pen registers, and traps and traces). In very limited emergency situations, specially designated law enforcement officials may request and obtain the installation and use of a pen register, or trap and trace device, before getting a court order. The present criteria in 18 U.S.C. § 3I25(a) require that:

a. the requesting law enforcement official have received "special designation" (which should be documented) from the U.S. Attorney General, the Deputy U.S. Attorney General, the Associate U.S. Attorney General, any Assistant U.S. Attorney General, any acting Assistant U.S. Attorney General, any Deputy Assistant U.S. Attorney General, or the principal prosecuting attorney of a State or State subdivision (county or city);

b. an emergency situation exists involving immediate danger of death or serious

physical injury to any person, or conspiratorial activities characteristic of organized crime; and

c. a court order approving the installation and use of the pen register, or trap and trace device, is issued within 48 hours after its installation.

6.4 Foreign Intelligence Surveillance Act. The U.S. Attorney General may authorize the employment of electronic surveillance to obtain foreign intelligence information if he or she reasonably determines that an emergency situation exists. The present criteria in 50 U.S.C. Sec. 1805(e) require that:

a. the U.S. Attorney General or his or her designee inform one of the seven U.S. District Court judges having jurisdiction over foreign intelligence surveillance activities as soon as possible; and

b. a court order approving the electronic surveillance be obtained within 24 hours after the Attorney General's authorization.

6.5 Future Statutory Changes. The foregoing descriptions of exigent circumstances permitting the initiation of electronic surveillance without a court order are based upon the Omnibus Crime Control and Safe Streets Act of 1968, and the Electronic Communications Privacy Act of 1986 (18 U.S.C. *§§* 2510-20, 2701-10 and 3121- 26), and the Foreign Intelligence Surveillance Act (50 U.S.C. *§§* 1801-11), as they existed on December 22, 2006. Future changes in these statutes, or their judicial interpretation, may modify the circumstances and requirements applicable to emergency situations.

7.0 Activation and Implementation of an Electronic Surveillance.

7.1 Review Credentials of Law Enforcement Official. Upon being presented with a court order or other authorization for the activation and implementation of an interception of communications or access to call identifying information, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager must confirm the identity of each of the law enforcement official(s) presenting the authorization. He or she must obtain: (a) the name of each law enforcement official; (b) the name of the law enforcement agency by which each official is employed; (c) the title or rank of each official; and (d) the badge number or similar identification number for each official. The Manager or Assistant Manager should request to photocopy the credentials for each official, and promptly do so if permitted. If not permitted to photocopy, the Manager or Assistant Manager must examine the credentials of each official, and make clear and written notes of the foregoing information from such credentials. The photocopy or notes must be attached to the Certification prepared and executed by the Manager or Assistant Manager with respect to the surveillance (see Section 8.0).

7.2 Review of Court Order or Other Authorization. Once the identity of the law enforcement official(s) presenting the court order or other authorization is confirmed, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager must examine the authorization itself, and determine if it is what it purports to be. As detailed in Section 5.0 above, the Manager or Assistant Manager may not conduct his or her own "judicial type" review of the validity of the authorization, but rather must make a reasonable determination whether the authorization appears to be valid on the basis of the inclusion or non-inclusion of most or all of the elements required by statute to be included in authorizations for the requested type of surveillance. The Manager or Assistant Manager should request to photocopy the court order or other authorization, and promptly do so if permitted. If the photocopy request is refused, the Manager or Assistant Manager must make clear and written notes of the following information: (a) the identity of the law enforcement official presenting the court order or other authorization; (b) the name of the person signing the court order or other authorization; (c) the type of interception of communications or access to call identifying information (e.g., Title III wiretap, pen register, trap and trace, Foreign Intelligence Surveillance Act); (d) the telephone number(s) or circuit identification numbers involved; and (e) the start date and time of the opening of the circuit for law enforcement. The photocopy or notes must be attached to the Certification prepared and executed by the Manager or Assistant Manager with respect to the surveillance (see Section 8.0). In addition, photocopies

or notes regarding any extensions of the court order or other authorization must be attached to that Certification.

7.3 Special Additional Procedures for Exigent Circumstances. Where a law enforcement official is requesting to activate a surveillance without a court order pursuant to a "special designation" from the U.S. Attorney General, a Deputy or Associate U.S. Attorney General, or the principal local state prosecuting attorney, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager must also inspect the "special designation" document giving the official the authority to do so. The Manager or Assistant Manager should request to photocopy the "special designation" document, and promptly do so if permitted. If the photocopy request is refused, the Manager or Assistant Manager must make clear and legible notes of the following information: (a) the date of the "special designation" document; (b) the name and title of the individual executing the "special designation" document; (c) the name and title of official receiving the "special designation"; (d) the specific, stated purpose of the "special designation"; and (e) the specific, stated powers granted to the official under the "special designation." The photocopy or notes must be attached to the Certification prepared and executed by the Manager or Assistant Manager with respect to the surveillance (see Section 8.0). In addition, the Manager or Assistant Manager must: (a) inquire from the official the reason for the emergency activation and implementation of the surveillance without a court order, and determine whether the stated reason constituted one of the exigent circumstances applicable to the type of surveillance requested (see Section 6.0 above); and (b) make arrangements to review and terminate the surveillance if a court order is not requested or obtained within the required time period for the type of surveillance (see Section 6.0 above).

7.4 Determination of Technical Feasibility. Once the existence of appropriate legal authorization has been determined, the CALEA Compliance Manager or "on duty" Assistant CALEA Compliance Manager must determine whether the requested interception of communications or access to call identifying information can be implemented technically. This step includes a determination by the Compliance Manager or Assistant Compliance Manager whether the court order or other authorization is sufficiently and accurately detailed to enable Carrier to comply with its terms. If the Manager or Assistant Manager cannot make this determination on the basis of the information furnished in the authorization and of his or her knowledge of the Carrier's network and facilities, he or she may consult first with the requesting law enforcement officials, and then (if necessary) with Carrier's technical employees and/or Carrier's switch vendor. In the latter instances, the Manager or Assistant Manager must not disclose any information to technical employees or vendor representatives that would compromise the security of the requested wiretap, pen register, trap and trace, or other electronic surveillance mechanism.

7.5 Actual Activation and Implementation of Surveillance. Once appropriate legal authorization and technical feasibility are established, the CALEA Compliance Manager or Assistant CALEA Compliance Manager will implement the requested interception of communications or access to call-identifying information and activate it at the date and time specified in the court order or other authorization, or as soon as possible thereafter. If the Manager or Assistant Manager is not technically capable of implementing or activating the interception or access personally, he or she will directly supervise the performance of the necessary technical functions by one of Carrier's technical employees. In the latter instance, the Manager or Assistant Manager will not disclose any more information than absolutely necessary for the technical employee to perform the necessary functions, and will maintain the security of the requested wiretap, pen register, trap and trace, or other electronic surveillance mechanism.

8.0 Preparation and Execution of Certification.

8.1 Same Day Preparation. The CALEA Compliance Manager or Assistant CALEA Compliance Manager implementing and activating (or directly supervising the implementation and activation of) an interception of communications or access to call-identifying information must prepare and execute a Certification in the form attached as Exhibit C before leaving the Carrier's premises on the day that the interception or access is implemented and activated.

8.2 Contents of the Certification. The required Certification must contain the following

information: (a) the identity of the law enforcement official presenting the court order or other authorization; (b) the name of the person signing the court order or other authorization; (c) the type of interception of communications or access to call identifying information (e.g., Title III wiretap, pen register, trap and trace, Foreign Intelligence Surveillance Act); (d) the telephone number(s) or circuit identification numbers involved; (e) the start date and time of the opening of the circuit for law enforcement; and (d) the telephone number(s) or circuit identification numbers involved; (e) the start date and time of the opening of the circuit for law enforcement; and (f) the name of the senior officer or employee of the Carrier (i.e., the CALEA Compliance Manager or Assistant CALEA Compliance Manager) who is responsible for overseeing the interception of communications or access to call- identifying information and who is acting in accordance with the Carrier policies and procedures established to comply with Section 64.2103 of the FCC Rules.

8.3 Attachments to the Certification. The CALEA Compliance Manager or Assistant CALEA Compliance Manager preparing the Certification must attach to it any photo copies obtained of the credentials of the requesting law enforcement official(s), of the court order or other legal authorization, and of any "special designation" document. The Manager or Assistant Manager also must attach to the Certification any notes prepared in lieu of, or addition to, photocopies.

8.4 Execution of the Certification. The CALEA Compliance Manager or Assistant CALEA Compliance Manager implementing and activating (or directly supervising the implementation and activation of) the interception of communications or access to call-identifying information must execute the Certification by signing Exhibit C before leaving the Carrier's premises on the day that the interception or access is implemented and activated. By his or her signature, the Manager or Assistant Manager is certifying for all relevant legal purposes that the Certification record is complete and accurate.

8.5 Security of Certification. The CALEA Compliance Manager will keep all completed and executed Certifications in a secure, locked file or filing cabinet where they may be accessed only by the CALEA Compliance Manager and by the Carrier's General Manager. If an Assistant CALEA Compliance Manager is not able to furnish his or her completed and executed Certification immediately to the CALEA Compliance Manager, he or she will keep the Certification in a secure and locked drawer or file until such time as it can be delivered to the CALEA Compliance Manager.

8.6 Review by CALEA Compliance Manager. The CALEA Compliance Manager will review all Certifications prepared and executed by the Assistant CALEA Compliance Manager(s). The Manager is responsible for investigating and resolving any problems or discrepancies with regard to the implementation or activation of the interception of communications or access to call-identifying information, or with regard to the preparation and execution of the Certification.

9.0 Security Breaches and Unauthorized Surveillance.

9.1 Prevention of Security Breaches. The CALEA Compliance Manager is Carrier's Primary Point of Contact with law enforcement, and will be the only Carrier officer or employee aware of the details of most interceptions of communications or access to call-identifying information. Only when the Manager is away or otherwise unavailable will an Assistant CALEA Compliance Manager become involved as the Carrier's Secondary Point of Contact with law enforcement. No Carrier officer or employee not expressly appointed as a CALEA Compliance Manager or an Assistant CALEA Compliance Manager may have any substantive contact with law enforcement regarding interceptions of communications or access to call identifying information, and must refer any inquiries or requests immediately to the Manager or (in his or her absence) an Assistant Manager. The Manager or Assistant Manager may, on occasion, consult with technical employees regarding technical feasibility, or supervise the actual physical installation of intercepts or access by technical employees, but will not disclose to them any information that is not absolutely necessary and that might compromise the security of the interception or access. All Certification records are kept in locked areas capable of being accessed only by the Manager and the Carrier's General Manager.

9.2 Reporting of Security Breaches. Any officer or employee of Carrier (including an Assistant CALEA Compliance Manager) who suspects for any reason that the security of a lawful interception of communications or access to call-identifying information has been compromised to unauthorized

persons or entities must notify the CALEA Compliance Manager as soon as possible (and no later than the same day). The Manager will investigate the matter immediately, and determine whether there is reason to believe that security was in fact compromised. If such reason exists, the Manager will notify the Carrier's General Manager, and will report the suspected breach of security to the law enforcement agency that requested the interception or access (unless this agency is believed to be involved in the breach of security, in which case the Manager will report the suspected breach of security to the Federal Bureau of Investigation or the U.S. Attorney General). The Manager will complete the investigation and report any suspected breach of security to the appropriate law enforcement agency as soon as possible, and in no event more than five (5) business days after the matter was brought to the Manager's attention.

9.3 Unlawful Electronic Surveillance. Unlawful electronic surveillance may occur for a variety of reasons, including: (a) the activation of interceptions or access by law enforcement without the affirmative intervention of an authorized officer or employee of a carrier (including the intervention of an unauthorized officer or employee); (b) the activation of interceptions or access on the basis of invalid court orders or other authorizations proffered by authorized or unauthorized law enforcement officials; and (c) the activation of interceptions or access without court orders on the basis of representations of exigent circumstances, and the subsequent failure of the requesting law enforcement official to apply for or obtain a court order within the required time period.

9.4 Reporting of Unlawful Electronic Surveillance. Any officer or employee of Carrier (including an Assistant CALEA Compliance Manager) who suspects for any reason that an unlawful electronic surveillance has occurred, or is occurring, on the Carrier's premises must notify the CALEA Compliance Manager at soon as possible (and no later than the same day). The Manager will investigate the matter immediately, and determine whether there is reason to believe that an unlawful electronic surveillance has in fact occurred, or is occurring. If such reason exists, the Manager will notify the Carrier's General Manager, and will report the suspected unlawful electronic surveillance to the Federal Bureau of Investigation (unless it is clear that a state or local law enforcement agency has jurisdiction over the matter). The Manager will complete the investigation and report any suspected unlawful electronic surveillance to the appropriate law enforcement agency as soon as possible, and in no event more than five (5) business days after the matter was brought to the Manager's attention.

10.0 Retention of Records.

10.1 Retained Records. The only records retained by Carrier regarding interceptions of communications and access to call-identifying information are the completed and executed Certifications, court orders, and other records for (a) authorized and unauthorized call content interceptions; and (b) authorized and unauthorized access to call-identifying information described in Section 8 above and Exhibit C.

10.2 Security of Records. The CALEA Compliance Manager will keep all completed and executed Certifications, court orders, and other records for (a) authorized and unauthorized call content interceptions; and (b) authorized and unauthorized access to call-identifying information in a secure, locked file or filing cabinet where they may be accessed only by the CALEA Compliance Manager and by the Carrier's General Manager.

10.3 Retention Period. Completed and executed Certifications, court orders, and other records for (a) authorized and unauthorized call content interceptions; and (b) authorized and unauthorized access to call-identifying information will be retained by the Carrier for a period of ten (10) years after the execution date.

EXHIBIT A

Primary and Secondary Points of Contact

Carrier's CALEA Compliance Manager and Primary Point of Contact

Name & Title	Business Phone	Cell Phone	Home Phone	FAX	Email Address

Carrier's Assistant CALEA Compliance Managers and Primary Points of Contact

Name & Title	Business Phone	Cell Phone	Home Phone	FAX	Email Address

EXHIBIT B

APPOINTMENT FORM

On behalf of _____, _____ is hereby appointed as its CALEA Compliance Manager for a period of time commencing on, _____ and extending indefinitely until terminated by a separate future action that will be noted at the bottom of this Appointment Form.

The job function of CALEA Compliance Manager is fully described in Section 3.0 of the Company's CALEA Compliance Policies and Procedures. It includes serving as the Point of Contact with law enforcement regarding wiretaps, pen registers, traps and traces, and other electronic surveillance activities; reviewing court orders and other authorizations for such activities; implementing properly authorized surveillance measures; remaining familiar with relevant federal and state statutes regarding authorization of electronic surveillance measures (including those involving exigent circumstances); reporting unauthorized activities and security breaches promptly to law enforcement; and preparing and retaining an appropriate certification record for each electronic surveillance.

The Appointee is aware that Communications Assistance for Law Enforcement Act compliance activities may occur only sporadically, and that no CALEA requests may be made by law enforcement for months or years at a time. However, when a CALEA request is made, it is likely to have very serious repercussions for the lives and safety of the public, as well as for the privacy rights of certain individuals or groups.

This APPOINTMENT is made this _____ day of _____, 20__.

_____ _____
Signature Title

This APPOINTMENT is accepted this _____ day of _____, 20__.

_____ _____
Signature Title

This APPOINTMENT is terminated this _____ day of _____, 20__.

_____ _____
Signature Title

EXHIBIT C

CALEA CERTIFICATION

CALEA CERTIFICATION

I, _____, hereby certify that I have been duly authorized to serve as the CLAEA Compliance Manager of the El Reno Municipal Authority, 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:

Start: Date _____ Time _____

Served by: Name _____ Agency _____

Issued By: Court _____ Docket/File No. _____

Judge _____

Law Enforcement Officer(s) Authorized to Receive Information:

Name_____ Agency _____

Name_____ Agency _____

Subscriber Name: _____

Telephone No./Circuit ID: _____

Type of Electronic Surveillance: ___ Pen Register ___ Trap & Trace ___ Title III

___ FISA ___ Other ___Placed at Office/Tandem

Supervising Employee

Name_____ Title _____

Other Employee(s)

Name_____ Title _____

Received Date _____ Time _____

Information Provided:

Date _____ Time _____

Extension request(a) ___ Yes ___No

Renewal Date: _____ Disconnection Date: _____
Renewal Date: _____ Disconnection Date: _____

Certification Attached:

EXHIBIT D

EMERGENCY SURVEILANCE REQUEST FORM

Name: _____

Title: _____

LEA Name: _____

Contact: _____

_____

Subject: Emergency Technical Assistance

I certify that I am specifically designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or the principal prosecuting attorney of the state or subdivision thereof acting pursuant to a statute of that state to command technical assistance from this telecommunications carrier in this emergency situation.

I have determined that an "emergency situation" exists that involves immediate danger of death or serious physical injury, conspiratorial activities threatening the national security interest, conspiratorial activities characteristic of organized crime, or an ongoing attack on a protected computer and requires this telecommunications carrier to provide technical assistance before an appropriate order can, with due diligence, be obtained from the court.

There are legal grounds upon which a court order could be obtained to authorize such electronic surveillance and direct this telecommunications carrier to provide all information, facilities and technical assistance.

An application for an order will be made within48 hours of receipt of this certification, or the time period provided by applicable law, and that this emergency electronic surveillance will cease if an order is not issued within this time period, the communication sought is obtained, or the application for an order is denied, whichever is earlier. This telecommunications carrier is hereby commanded to provide technical assistance for _____.

No legal cause of action shall lie against this telecommunications carrier for complying in good faith with this certification.

Signed:_____ Date: _____

Time:_____