Advanced Communications Technology, Inc. ("ACT")

CALEA SECURITY COMPLIANCE MANUAL

Questions concerning compliance with the policies and procedures in this area should be referred immediately to:

Dave Berry
Operations Manager
Phone: 307.673.0910
E-mail: dberry@acthq.net

These policies and procedures will remain in effect until further notice.

Dated March 27, 2019

Aaron Sopko
General Manager

Revisions to Manual Format:

Revision	Date	Resp.	Reason
11	3/27/2019	ACT	Replaces manual dated March 7, 2011 to edit contact procedures in Section 5 and to update contacts on this page and in Attachment A.

Table of Contents

Attachments:

1. Purpose

Section 105 of the Communications Assistance for Law Enforcement Act (CALEA) requires, inter alia, that each company take steps to ensure any interception of communications or access to call identifying information be activated by the company only in strict accordance with a court order or other form of lawful authorization. Such action shall only occur when directed by the authorized employees of ACT.

CALEA empowers the Federal Communications Commission (FCC) with the authority to promulgate such rules as are necessary to implement the provisions of Section 105. ACT's policy regarding the use of wiretaps and surveillance methods and procedures has been modified to reflect current rules in effect.

For the purpose of this CALEA Security Compliance Manual (Manual) and all Attachments hereto, the term "Company" shall refer to ACT, and may be either singular if the Manual is filed for one entity, or plural if the Manual is filed for multiple entities.

2. Overview

ACT employees that receive a request from law enforcement agencies or any other authorized party, for any form of electronic surveillance, wiretaps, customer calling information, or information that is deemed Company private or customer specific must follow these procedures exactly. Employees acting outside of these procedures and not adhering to these instructions may face possible disciplinary actions up to and including dismissal.

3. Definitions

For purposes of these CALEA compliance procedures only, the definitions applicable are as follows:

"Appropriate legal authorization" shall include and be limited to:

(1) A court order signed by a judge or magistrate authorizing or approving the interception; or

(2) Other authorization to 18 U.S.C. §2518 (7), or any other relevant federal or state statue.

"Appropriate company authorization" means the policies and procedures adopted to supervise and control employees authorized to assist law

enforcement in conducting any interceptions for communications or access to call identifying information. The authorized employee(s) must receive appropriate legal authorization and appropriate company authorization before enabling law enforcement officials and designated company personnel to implement the interceptions of communications or access to call-identifying information.

"Call content interception" means an interception of a communication, including the content of the communication. An example is a court ordered wiretap, issued in accordance with the provisions of Title III.

"Call identifying information interception" means the act of 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 the equipment, facilities, or service of this Company. An example of this activity is a pen register or trap-and-trace surveillance.

"Collection function" is the location where lawfully authorized intercepted communications and call identifying information is collected by a law enforcement agency.

"Content of subject- initiated-conference calls" is the capability that permits a law enforcement agency to monitor the content of conversations by all parties connected via a conference call when the facilities under surveillance maintain a circuit connection to the call.

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

"Dialed digit extraction" is the capability that permits a LEA to receive on the call data channel digits-dialed by a subject after a call is connected to another company's service for processing and routing.

"Direction" is a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., a redirected-to party or redirected-from party).

"FISA" is the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1843.

"Intercept Access Point (IAP)" is a point within the Company's system where some of the communications or call-identifying information of an intercept subject's equipment facilities and services are accessed.

"In-band and out-of-band signaling" is the capability that permits a LEA to be informed when a network message that provides call identifying

information (e.g., ringing, busy, call waiting signal, message light) is generated or sent by the IAP switch to a subject using the facilities under surveillance. Excludes signals generated by customer premises equipment when no network signal is generated.

Law Enforcement Agency (LEA) means any officer of the United States, or of a state or political subdivision who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in 18 U.S.C. § 2516, as may be amended from time to time, or under applicable state or locality statutes, any attorney authorized by law to prosecute or participate in the prosecution of such offenses, or authorized by law to apply to the Foreign Intelligence Surveillance Court for authorization to engage in electronic surveillance under the Foreign Intelligence Surveillance Act.

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

"Party hold, drop on conference calls" is the capability that permits a LEA to identify the parties to a conference call conversation at all times.

"Pen register" is defined in 18 U.S.C. § 3127 (3) to be '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 communication 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.'

"Subject-initiated dialing and signaling information" is the 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" is 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).

"Timing information" is a capability that permits a LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the Company's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the

time, and with the call event time-stamped to an accuracy of at least 200 milliseconds.

"Title III" refers to Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

4. Job Functions of Authorized Points of Contact

4.1 Primary Point of Contact

ACT's CALEA Primary Point of Contact noted in Attachment A is appointed at the discretion of the VP/General Manger. ACT's Primary Contact is responsible for interaction with law enforcement officials and agencies regarding all CALEA related matters. Examples of such 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 wiretaps, pen registers, traps and traces, or other electronic surveillance measures, and making 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 wiretaps, pen registers, traps and traces, or other electronic surveillance measures, and determining whether the specially requested measures can be implemented technically;

d. Implementing (or overseeing the implementation by a competent technical employee) of properly authorized (that is, those having both appropriate legal authorization and appropriate Company 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;

f. Reporting any and all acts of unauthorized or unlawful electronic surveillance occurring on ACT's premises to the appropriate law enforcement agency within a reasonable time period (not to exceed five (5) 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 (5) business days) after their discovery;

h. Preparing and signing a complete and accurate certification for each and every wiretap, pen register, trap and trace, or other electronic surveillance measure implemented by ACT;

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 ACT for a period of ten years (10) after the termination of the surveillance measure;

j. Reviewing and revising, if necessary, the present CALEA Security and Compliance Manual after significant changes federal or state electronic surveillance statutes, or relevant FCC rules; and

k. Reviewing and revising if necessary, the present CALEA Security and Compliance Manual after significant change in ACT operating policies, job functions, or personnel authorized to deal with CALEA-related matters to include the most current information regarding contact of personnel responsible for and trained in wiretaps, pen registers, traps and traces, or other electronic surveillance implemented by ACT.

l. Training and supervising the activities of Secondary Point(s) of Contact as noted in Attachment A.

m. Implementing (or overseeing the implementation by a competent employee) of a system of classification and retention for all information and records that result from:

    1.) Properly authorized (that is, those having both appropriate legal authorization and appropriate Company authorization) wiretaps, pen registers, traps and traces, or other electronic surveillance measures and/or:
    2.) Any breaches of security or compromise of any electronic surveillance that is conducted by the company.

4.2 Secondary Contacts

ACT's Secondary Contact(s) are appointed at the discretion of the Primary Contact or VP/General Manager. Secondary Contacts are responsible for interacting with law enforcement officials and agencies regarding CALEA-related matters when the Primary Contact is unavailable. The duties are the same as those for the Primary Contact until the Primary Contact is available.

5. Contact Procedures

CARRIER PERSONNEL MUST RECEIVE APPROPRIATE LEGAL AUTHORIZATION AND APPROPRIATE CARRIER AUTHORIZATION AS DEFINED IN SECTION 3 OF THIS MANUAL BEFORE ENABLING LAW ENFORCEMENT OFFICIALS AND CARRIER PERSONNEL TO IMPLEMENT THE INTERCEPTION OF COMMUNICATIONS OR ACCESS TO CALL-IDENTIFYING INFORMATION

Any Company employee receiving a request for electronic surveillance, wiretap or customer specific information from anyone, law enforcement or otherwise, must immediately direct the requesting party to the Company's General Manager and Primary Contact, or, in their absence, to the appropriate Secondary Contact(s) as identified in Attachment A, who have been designated by this Company as the only authorized persons to accept these requests and act on them. These authorized Company employees will be specifically charged with the responsibility to assist law enforcement, or other authorized agency, in conducting any interception of communications or access to call-identifying information and will be responsible for determining that "appropriate legal authorization" has been received. If there is a question about what is being requested and the Company's duty to comply with the request, the authorized Company employees shall contact the Company's Chief Regulatory Officer and/or legal counsel. For requests with respect to issues addressed in this CALEA Manual, the authorized Company Employees shall comply with the procedures set forth in this CALEA Manual. For all other law enforcement requests, the Company shall comply with the applicable legal requirements for those requests including, if applicable, via separate policies and procedures the Company may have for compliance with those requests. Nothing in this CALEA Manual precludes the Company from contracting with a third-party vendor to implement properly authorized wiretaps, pen registers, traps and traces, or other electronic surveillance measures subject to the compliance with this CALEA Manual by the third-party vendor.

5.1 Availability

ACT is a small company with a limited number of employees, and is not staffed at all times. The contacts noted in Attachment A may not be available at all times. For requests for surveillance, all Company personnel and law enforcement agencies should use the following procedures:

5.1.1 Business Hours

During ACT's normal business hours, the employees greeting visitors at a main business office and the employees answering ACT'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 Company's Primary

Contact, or, in his or her absence, to the appropriate Secondary Contact(s) as identified in Attachment A. If the Primary or Secondary Contact(s) is not immediately available, they should be paged and the call returned within ½ hour.

5.1.2 Non-Business Hours

At all times when the ACT'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 Company's technician on duty. The technician on duty will contact the Company's Primary Contact, or, in his or her absence, to the appropriate Secondary Contact(s) as identified in Attachment A.

6. Subpoenas/Court Orders: Processing

A subpoena/court order can be served via facsimile to the authorized Point(s) of Contact. The facsimile number is found on Attachment A. An original copy of the subpoena/court order must be provided within 48 hours of the facsimile, via US Mail, courier or by express delivery service. The original copy will be held as the retention document, in addition to the fax copy.

Routing subpoenas for subscriber information and/or call records are processed in the order in which they are received. As a general rule, responses are returned to the requesting party (by facsimile or email) within three (3) business days.

Court orders requesting "Pen Register/Trap and Trace", or content surveillance ("Title III") receive priority treatment. An example of a basic court order is found as Attachment D.

7. Appropriate Authorization

7.1 Definition of "Appropriate Authorization"

No interception of communications or access to call-identifying information may be implemented or activated on ACT's premises without appropriate legal authorization. Further, interception of communications or access to call-identifying information may be implemented or activated on ACT's premises solely by Company personnel who have appropriate Company authorization.

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. Sec. 2518(7) or any other applicable federal or state statute.

7.2 Documents Indicating "Appropriate Legal Authorization"

The Company 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. A document which reasonably appears to be a valid court order authorizing the interception of wire or electronic communications, the installation and use of a pen register or a trap and trace device, or electronic surveillance under the Foreign Intelligence Surveillance Act (FISA); or

b. A document which reasonably appears to be a valid indication that the requesting law enforcement official is a specially designated representative of the US Attorney General, a Deputy Attorney General, Associate Attorney General or principal federal or state prosecuting attorney for the area.

7.3 Documents Indicating "Appropriate Company Authorization"

Only those employees identified on Attachment A (as part of this Manual) have received official authorization to assist law enforcement in their conduct of interceptions for communication or access to call identifying information.

8. Reasonable Determination of Appropriate Legal Authorization

8.1 Interception of Communications (wiretaps)

In reviewing a court order authorizing or approving a wiretap to determine whether it is what it purports to be, ACT's designated Contact(s) 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 (US Court of Appeals, US District Court or state court having general criminal jurisdiction) for the circuit or district in which the Company 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(s) 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 communications 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 court order;

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

i. A statement whether or not the interception will automatically terminate when the described communications are first intercepted and obtained;

j. A directive that the Company 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 ACT 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 (optional, at the issuing judge's discretion) 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.

8.2 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 Company Point(s) of Contact 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 (US Court of Appeals, US District Court or state court having general criminal jurisdiction) for the circuit or district in which the Company 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 law enforcement agency authorized to use the call-identifying information;

g. The name of the law enforcement official authorizing the application for the court 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 Company 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.

9. Emergency Circumstances When No Court Order May Be Required

9.1 Exigent or Emergency Circumstances

In some cases, due to the emergency nature of the request, and the imminent threat to life, property, or national security, law enforcement may request surveillance without a court order. To obtain such surveillance, the law enforcement agency shall present to ACT a request for an emergency surveillance signed by the Attorney General of the United States (or an Assistant Attorney General of the United States) for federal law enforcement, or the Attorney General of the State of Wyoming for state law enforcement.

For all emergency surveillances initiated based on a letter from the appropriate Attorney General, the law enforcement agency shall present ACT with a valid court order for the surveillance, signed by a judge with the appropriate jurisdiction within 48 hours of the inception of the surveillance. If such court order is not provided within 48 hours, ACT will terminate the surveillance.

9.2 Surveillance Prior to Receipt of Court Order

It is legal for ACT to conduct surveillance at the request of law enforcement prior to receiving court order. This normally occurs from ransom calls in kidnapping or extortion cases. ACT will provide the results of the surveillance to law enforcement only when law enforcement has produced a valid court order for the surveillance, signed by a judge with the appropriate jurisdiction.

9.3 One Party Consent

It is legal for ACT to conduct surveillance at the request of law enforcement when one party to the surveillance has given consent. Such surveillance will be conducted only at the request of law enforcement, not upon request of the consenting party to ACT. The Company will provide results of the surveillance to law enforcement only when law enforcement has provided a valid court order for the surveillance, signed by a judge within the appropriate jurisdiction.

10. Technical Feasibility

ACT's Point(s) of Contact must determine whether the court order or other authorization is sufficiently and accurately detailed to comply with its terms. If this determination can not be made on the basis of the information furnished in the authorization, the Company will consult first with the requesting law enforcement official(s), and then (if necessary) with the Company's technical employees and/or switch vendor. In the latter instances, the Company will 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.

10.1 Activation and Implementation of Surveillance

Once appropriate legal authorization and technical feasibility are established, the Company's Point(s) of Contact 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 Point(s) of Contact 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 the Company's technical employees. In the latter instance, the Point(s) of Contact 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.

11. Security Breaches and Unauthorized Surveillance

11.1 Prevention of Security Breaches

The Company's Primary Contact with law enforcement will be the only officer or employee of the Company aware of the details of most interceptions of communications or access to call-identifying information. Only when the Primary Contact is unavailable will other designated Secondary Contact(s) become involved with law enforcement. No Company officer or employee not formally appointed as a Point of Contact 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 designated Point(s) of Contact. The designated contacts 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.

No employee except the designated Point(s) of Contact who has any knowledge of an electronic surveillance, regardless of whether this knowledge was obtained from direct involvement or from a second party contact, may reveal any such knowledge of the surveillance whether to law enforcement agencies, other employees of the company, or any third party not employed by the company.

All records are kept in locked areas capable of being accessed only by the Primary Contact.

11.2 Reporting of Security Breaches

Any officer or employee 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 Primary Contact or VP/General Manager as soon as possible (and no later than the same day).

The Primary Contact or VP/General Manager will investigate the matter immediately, and determine whether there is reason to believe that security was in fact compromised. If such reason exists, this individual 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 Primary Contact or VP/General Manager will report the suspected breach of security to the Federal Bureau of Investigation or the US Attorney General).

The Primary Contact or VP/General Manager will then 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 Primary Contact's or VP/General Manager's attention. A record will be completed using Attachment C.

11.3 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 the Company (including the intervention of an unauthorized officer or employee); (b) the activation of interceptions or access on the basis of invalid or no court orders or other authorizations proffered by authorized or unauthorized law enforcement officials; and/or (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.

11.4 Reporting of Unlawful Electronic Surveillance

Any officer or employee who suspects for any reason that an unlawful electronic surveillance has occurred, or is occurring, on the Company's premises must notify the Primary Contact or VP/General Manager as soon as possible (and no later than the same day).

The Primary Contact or VP/General 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 Primary Contact or VP/General Manager will report the suspected unlawful electronic surveillance as soon as possible to the Federal Bureau of Investigation (unless it is clear that a state or local law enforcement agency has jurisdiction over the matter).

The Primary Contact or VP/General Manager will then 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 Primary Contact's or VP/General Manager's attention. A record will be completed using Attachment C.

11.5 Unauthorized Use of Surveillance Capabilities

Any employee who knowingly misuses the Company's capabilities to provide electronic surveillance in such manner as to cause or assist in the cause of a

a.) Breach of security
b.) Unlawful electronic surveillance, or,
c.) False reporting of breaches of security or unlawful surveillance

whether to law enforcement agencies, other employees of the company, or any third party not employed by the company, will face severe disciplinary measures up to and including dismissal.

12. Record Retention

All information regarding a lawful request or any other request for interception and/or call content information will be documented on a Company approved certification form at the time of the request or as soon as possible thereafter, not to exceed forty-eight (48) hours, and will include at least the following information:

a. The signed and dated court order, and the name and department of the presenting law enforcement officer, including an address and wireline telephone number; [see Attachment B].

b. In the case of an unauthorized request, a written document detailing the request, with the signature of another authorized employee; [see Attachment C].

c. Telephone number(s) and or circuit identification numbers involved; start date and time of the opening of the circuit for law enforcement officers; identity of the law enforcement officer presenting the authorization; the type of interception of communications or access to call identifying information (e.g., pen register, trap and trace, Title III, FISA); the name of the person signing the appropriate legal authorization; the name of the Company employee who is responsible for overseeing the interception of communications or access to call identifying information; and all documentation supporting the request must be attached to the completed Company approved form; [see Attachment B or C].

d. After review of the Company approved form and associated documents, the Primary Contact will sign and date the record certifying that the record is complete and accurate, and ensure that all authorized requests and supporting information are placed in a secure area for a period of ten (10) years.

DESIGNATED EMPLOYEE INFORMATION

Employees designated as contacts for law enforcement personnel are available on a 24-hour basis. Only designated employees are authorized to implement interceptions. See Page 2 of Attachment A for additional contact procedures.

Primary Contact Name: Dave Berry
Position/Title: Operations Manager

Contact Information: Tel: 307.673.0910
Fax: 307.673.0911
Cell: N/A
Email: dberry@acthq.net

Secondary Contact Name: Aaron Sopko
Position/Title: Vice President/General Manager

Contact Information: Tel: 307.673.0910
Fax: 307.673.0911
Cell: 307.431.9075
Email: sopko@acthq.net

Secondary Contact Name: Jason Gardner
Position/Title: Data Network Supervisor

Contact Information: Tel: 307.673.0910
Fax: 307.673.0911
Cell: 307.752.7156
Email: jgardner@acthq.net

Secondary Contact Name: Rob Johnson
Position/Title: Business Development Manager

Contact Information: Tel: 307.673.0910
Fax: 307.673.0911
Cell: 307.752.9369
Email: rob.johnson@acthq.net

Primary Contact Name: Zjon May
Position/Title: Engineering Supervisor

Contact Information: Tel: 307.673.0910
Fax: 307.673.0911
Cell: 406.351.2480
Email: zjon.may@acthq.net

DESIGNATED EMPLOYEE INFORMATION

ACT is a small company with a limited number of employees, and is not staffed at all times. The contacts noted in Attachment A may not be available at all times. For requests for surveillance, all Company personnel and law enforcement agencies should use the following procedures:

Business Hours

During ACT's normal business hours, the employees greeting visitors at a main business office and the employees answering ACT'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 Company's Primary Contact, or, in his or her absence, to the appropriate Secondary Contact(s). If the Secondary Contact(s) is not immediately available, he or she will be paged and the call returned within ½ hour.

Non-Business Hours

At all times when the Company'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 Company's technician on duty. The technician on duty will contact the authorized Point(s) of Contact as identified in Attachment A.

RECORD OF AUTHORIZED INTERCEPTION

This form should be completed before interception occurs. If you are unable to complete the form prior to interception, you must complete the form within 48 hours of implementation of authorized interception. A copy of the written authorization for implementation of the intercept must be attached with this form.

Employee name (must be authorized to perform interception) _____

Name(s) of additional employee(s) that assisted with the interception (must have signature below from each employee) _____
_____
_____

Employee(s) Position _____
_____
_____

Identity of Law Enforcement Officer presenting authorization _____

Contact Information for Officer listed above

_____

Law Enforcement Officer's Organization

_____

Badge Number (if applicable)

_____

Name of Judge or Prosecuting Attorney that signed authorization: _____

Telephone number(s) or Circuit identification numbers involved in interception _____

Type of interception (pen register, trap and trace, Title III FISA, etc.) _____

Start date and time of interception _____

Stop date and time of interception _____

As an employee designated to authorize and implement CALEA related activity, I hereby swear that I will not disclose any information about this interception to any person not properly authorized by statute or court order.

Employee signature	Date
Employee signature	Date
Employee signature	Date

RECORD OF UNAUTHORIZED INTERCEPTION

This form should be completed immediately upon detection of the possibility of an unauthorized interception with the data available at the time of detection. If such possibility exists, the Primary Contact will report the suspected unlawful electronic surveillance as soon as possible (but in no event more than five (5) business days after the matter was brought to the Primary Contact's attention) to the Federal Bureau of Investigation (unless it is clear that a state or local law enforcement agency has jurisdiction over the matter).

When the investigation of the possible unlawful interception is complete, complete the entire form and report as soon as possible (in no event more than five (5) business days after the completion of the investigation of the unauthorized interception) to the Federal Bureau of Investigation (unless it is clear that a state or local law enforcement agency has jurisdiction over the matter).

Employee name (must be authorized to perform interception) _____

Identity of Law Enforcement Officer notified of unauthorized interception _____

Contact Information for Officer listed above

_____

Law Enforcement Officer's Organization

_____

Badge Number (if applicable)

_____

Telephone number(s) or Circuit identification numbers involved in interception _____

Nature of unlawful interception (pen register, trap and trace, Title III FISA, etc.) _____

Start date and time of interception _____

Stop date and time of interception _____

As an employee of Advanced Communications Technology, Inc., I hereby swear that I will not disclose any information about the interception above to any person not properly authorized by statute or court order.

Employee signature	Date
Employee signature	Date
Employee signature	Date

Example of Court Order Submitted by a Law Enforcement Agency for a Call Information Intercept

IN THE MATTER OF THE APPLICATION BY {JURISDICTION} FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF A PEN REGISTER AND/OR TRAP AND TRACE

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 3122 by {**Name}**, an attorney for the Government, which application requests an order under Title 18, United States Code, Section 3122 authorizing the installation and use of a pen register and/or trap and trace on {**telephone number(s)}**, the Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of {**Specific Criminal Offense(s)}** by {**Person(s)}** and others as yet unknown.

IT APPEARING that the numbers dialed or pulsed from/to {**telephone number(s)}**, listed to or leased by {**name(s) of person(s)}**, and located at {**address**}, is/are relevant to an ongoing criminal investigation of the specified offenses,

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123 and 3124, that agents of {**Investigative Agency**} may install and use a pen register and/or trap and trace to register numbers dialed or pulsed from or to {**telephone number(s)**}, to record the date and time of such pulsing or recordings, and to record the length of time the telephone receiver(s) in question is/are off the hook for incoming or outgoing calls for a period of {**Not to Exceed 60 Days**}, and if trap and trace order, {**geographic limitations**}; and,

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3124, that {**Company**} shall furnish agents of the {**Investigative Agency**} forthwith all information, facilities and technical assistance necessary to accomplish the installation of the pen register and/or trap and trace unobtrusively and with minimum interference to the services that are accorded persons with respect to whom the installation and use is to take place; and,

Example of Court Order Submitted by a Law Enforcement Agency for a Call Information Intercept

IT IS FURTHER ORDERED, that {**Company**} be compensated by the applicant for reasonable expenses incurred in providing technical assistance; and,

IT IS FURTHER ORDERED, that {**Company**} shall supply {**Investigative Agency**} with subscriber information, including published and non-published telephone information, for those telephone numbers, names or addresses identified in this order and/or obtained by the pen register and/or trap and trace installed pursuant to this order and,

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123, that this order and the application be sealed until otherwise ordered by the Court, and that {**Company**}, its agents and employees shall not disclose the existence of the pen register and/or trap and trace, or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

JUDGE_____ DATE _____

NOTE: The above is a sample of a basic court order for a pen register or trap/trace. In addition to the above, the court order is to include other specifics required by law enforcement. A company cannot provide information that is not specified and required by the court order. Title III Wire Intercepts follow the same basic format; however, the timeframe cannot exceed 30 days.