



**WILTSHIRE
& GRANNIS** LLP

1200 18TH STREET, N.W., STE. 1200
WASHINGTON, D.C. 20036-2516
U.S.A.

TEL +1 202 730 1337
FAX +1 202 730 1301
WWW.WILTSHIREGRANNIS.COM
ATTORNEYS AT LAW

31 January 2011

BY ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Revised System Security and Integrity Plan of AST Telecom, LLC, and American Samoa License, Inc., d/b/a Blue Sky Communications, ET Docket No. 04-295

Dear Ms. Dortch:

As required by 47 C.F.R. § 1.20005, AST Telecom, LLC, and American Samoa License, Inc., d/b/a Blue Sky Communications submit their revised System Security and Integration (“SSI”) Plan. This SSI Plan supersedes the previous version dated and filed with the Commission on January 9, 2008.

Should you have any questions, please contact me by telephone at +1 202 730 1337 or by e-mail at kbressie@wiltshiregrannis.com

Respectfully submitted,

Kent D. Bressie
*Counsel for AST Telecom, LLC, and
American Samoa License, Inc.*

SYSTEMS SECURITY AND INTEGRITY PLAN
CALEA POLICIES AND PROCEDURES
FOR AST TELECOM, LLC, AND AMERICAN SAMOA LICENSE, INC.

REVISED MANUAL

January 31, 2011

(1) STATEMENT OF CORPORATE POLICY

It is the policy of AST Telecom, LLC and American Samoa License, Inc. (together, d/b/a Blue Sky Communications (“Blue Sky”)) to comply with letter and spirit of all laws of the United States, including the Communications Assistance for Law Enforcement Act (“CALEA”). Section 105 of CALEA requires a telecommunication carrier to ensure, before assisting a law enforcement agency to carry out a call content interception or a call information interception, that the interception is activated (1) pursuant to court order or “other lawful authorization,” and (2) with the “affirmative intervention” of a carrier officer or employee. 47 U.S.C. § 1004.

The Federal Communications Commission has issued regulations to implement section 105, see 47 C.F.R. §64.2100-.2106, and these regulations require that carriers create policies and procedures to govern, their electronic surveillance activities. This compliance Manual sets forth Blue Sky’s policies and procedures which constitute the appropriate legal and carrier authorization necessary for the appropriate authorization required to conduct electronic surveillance. Blue Sky recognizes that the unique technical design of GSM PCS systems may present unique issues in a CALEA environment. In such an event, Blue Sky’s CALEA Contact Officers (referred to herein also as “Designated Employee(s)” or “DE(s)”) will consult with the appropriate Law Enforcement Agency.

All employees are required to follow the policies and procedures specified in the Manual. The FCC is authorized under CALEA to punish violations of both its regulations and carriers’ internal surveillance policies and procedures. In addition, Title 18 of the United States Code authorizes civil damages, fines, and imprisonment for the unlawful interception or disclosure of wire and electronic communications.

Any questions about how to comply with the policies and procedures in this Manual should be referred to the Chief Executive Officer listed in Appendix A.

Any violation of or departure from the policies and procedures in this Manual shall be reported immediately to the Chief Executive Officer, listed in Appendix A.

(2) GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE

(a) “Appropriate Authorization” Required To Conduct Electronic Surveillance

It is the policy of Blue Sky to permit only lawful, authorized electronic surveillance to be conducted on its premises.

Blue Sky will supervise its personnel to ensure that any interception or access to call-identifying information is lawfully conducted. Employees shall have both “appropriate legal authorization” and “appropriate carrier authorization” before enabling law enforcement officials and carrier personnel to implement the interception of communications or to access call-identifying information. It shall be the responsibility of the Designated Employee(s) (“DE”) listed in Appendix A

to determine whether there is “appropriate legal authorization” and provide “appropriate carrier authorization” only if such “appropriate legal authorization” exists. However, if the DE determines that a condition envisioned in Section 2 or Section 5, exists, no court order will be required. Section 5 of this Compliance Manual sets forth how each form of authorization is to be obtained.

(b) Designated Employees/CALEA Contact Officers

- (i) Blue Sky hereby designates the CALEA Contact Officers listed in Appendix A.

(c) Responsibilities of CALEA Contact Officers or Designated Employees

- (i) The DE’s are hereby authorized by Blue Sky to implement lawful electronic surveillance in accordance with policies and procedures in this Manual and to delegate any tasks associated with the surveillance to other employees. The responsibilities to be undertaken by such employees are as follows:
 - (1) Oversee the implementation of each electronic surveillance conducted on the premises of Blue Sky;
 - (2) Responsible for assuring that he/she is fully apprised of all relevant state and federal statutory provisions affecting the legal authorization a carrier must have to conduct electronic surveillance, including section 2518(7) of Title 18 of the United States Code, which authorizes certain law enforcement personnel to conduct the interception of communications without a court order if an emergency situation exists involving:
 - (a) Immediate danger of death or serious physical injury to any person;
 - (b) Conspiratorial activities threatening the national security interest; or
 - (c) Conspiratorial activities characteristic of organized crime
 - (3) Reasonably intervene to make sure that there is appropriate legal authorization for each electronic surveillance, including any appropriate authorization required under relevant state and federal statutes.
 - (4) Complete Blue Sky’s Certification Form for each electronic surveillance he/she oversees and do so either contemporaneously with, or within a reasonable period of time after the initiation of, the surveillance.

- (5) Make sure that records for each surveillance are placed in the appropriate files.

All employees are prohibited from conducting any unauthorized surveillance and from disclosing to any person the existence of, or information about, any law enforcement investigation or electronic surveillance unless required by legal process and then only after prior notification to a representative of the Attorney General of the United States or to the principal prosecuting attorney of the state or subdivision thereof, as maybe appropriate.

Employees shall report any incidents of unauthorized surveillance and any compromises of authorized surveillance to the DEs.

The Director of Engineering and Operations listed in Appendix A. has been appointed to update this manual and direct the filing of the updated manual to the FCC within 90 days of any amendment.

(3) MAINTENANCE OF SECURE AND ACCURATE RECORDS

(a) Certification Form

An employee shall complete Blue Sky's Certification form (See Attached Exhibit 1) for every electronic surveillance conducted on Blue Sky's premises – regardless of whether the surveillance was authorized or unauthorized. The Certification will include the following Information:

- (i) telephone number(s) and/or circuit identification number(s) involved;
- (ii) start date and time that the carrier enables the interception of communications or access to call identifying information;
- (iii) identity of law enforcement officer with the authorization; iv) name of judge or prosecuting attorney; v) type of interception or access to information (i.e. pen register, trap and trace);
- (vi) name of the DE responsible for overseeing the interception or access to call-identifying information.

(4) MAINTENANCE OF RECORDS/RECORDS RETENTION PERIOD

(a) Blue Sky shall establish and label separate files in which it will retain all Certification Forms, court orders and other records for:

- (i) authorized call content interception;
- (ii) unauthorized call content interceptions; and
- (iii) authorized and unauthorized call information interceptions.

- (b) These records shall be retained in secure and appropriately-marked files accessible only to the CEO for ten years from the time Blue Sky's Certification Form is completed for the interception.
- (c) Records of call-identifying information and unauthorized interceptions (including the content of unauthorized interceptions) will be maintained for ten years.
- (d) Blue Sky will file policies and procedures with the FCC no later than 90 days after it has amended its existing policies and procedures.
- (e) Blue Sky will file policies and procedures with the FCC no later than 90 days after the effective date of a merger or divestiture in which it becomes the surviving or divested entity.

(5) PROCEDURES TO PREVENT UNAUTHORIZED INTERCEPTION OR ACCESS

(a) Call Content Interception with a Title III Court Order

The following steps will be taken by Blue Sky with respect to the integrity of its electronic surveillance system security:

- (i) Any court order presented by a law enforcement agency for a call content interception pursuant to Title III also known as "The Federal Wire Tap Act", shall be referred immediately to a DE.
- (ii) Before implementing the interception, the DE shall make sure that the court order contains the following information:
 - (1) the identity of the person, if known, whose communications are to be intercepted;
 - (2) the nature, and location of the communications facilities or the place for which authority to intercept is granted;
 - (3) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
 - (4) the period of time during which the interception is authorized, including a statement whether the interception shall automatically terminate when the described communication has been first obtained;
 - (5) a provision that the authorization to intercept shall be executed as soon as practicable and conducted in such a way as to minimize the

interception of communications not otherwise sufficient to interception; and

(6) the signature of a judge or magistrate.

(b) The DE shall determine whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable Blue Sky to comply with its terms.

- (i) Once the DE authorizes the implementation of the surveillance, the DE may delegate tasks associated with the surveillance to other employees, but the DE shall continue to oversee the implementation of the surveillance.
- (ii) The DE shall complete Blue Sky's Certification Form as soon as possible after the initiation of the electronic surveillance. The DE shall supply all information requested on Blue Sky's Certification Form that is not contained on the court order. Blue Sky's Certification Form. The DE also shall attach to Blue Sky's Certification Form any extensions that are granted for the surveillance by the Court.
- (iii) The DE shall make sure that Blue Sky's Certification Form and all attachments are given to the CEO for appropriate filing.
- (iv) The DE shall continue to oversee the conduct of the electronic surveillance and make sure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the court order (which, in the absence of an extension, cannot exceed 30 days).

(c) Call Content Interceptions Without a Court Order

- (i) Any request by a LEA for a call content interception without a court order, pursuant to the exigent circumstances listed in 18 U.S.C. § 2518(7), shall be referred immediately to the DE for review by the DE. No such request shall be granted unless the DE determines that it falls within the limited exceptions discussed in Section 2 or Section 5. Such a determination shall be reduced to writing, placed in the secure file and Blue Sky's Certification Form shall be completed.

(d) Steps to be Followed Prior to the Interception when there is not a Court Order.

- (i) Before implementing the interception, the DE shall make sure that the LEA provides a Certification ("LEA Certification") containing the following information:
 - (1) the information, facilities, or technical assistance required;

- (2) the period of time during which the provision of information, facilities, or technical assistance is authorized;
- (3) a statement that no warrant or court order is required by law;
- (4) a statement that all statutory requirements have been met; including, but not limited to, certification that the signatory is duly authorized;
- (5) a statement that the specific requested assistance is required; AND the signature of either:
 - (6) the Attorney General of the United States, or
 - (7) a law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any US Territory, State or subdivision thereof.
- (ii) The DE also shall determine whether the surveillance can be implemented technically AND whether the LEA Certification is sufficiently and accurately detailed to enable Blue Sky to comply with its terms.
- (iii) Once the DE authorizes the implementation of the surveillance the DE may delegate tasks associated with the surveillance to other employees, but the DE shall continue to oversee the implementation of the surveillance.
- (iv) The DE shall complete Blue Sky's Certification Form as soon as possible after the initiation of the electronic surveillance.
- (v) The DE shall supply information requested on Blue Sky's Certification Form that is not contained in the LEA Certification.
- (vi) The DE then shall attach the LEA Certification and sign Blue Sky's Certification Form.
- (vii) The DE shall make sure that Blue Sky's Certification Form and all attachments are given to the CEO for appropriate filing.
- (viii) The DE shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance as soon as any of the following events occur.
- (ix) the law enforcement agency does not apply for a court order with 48 hours after the interception has begun; or

(x) the law enforcement agency's application for a court order is denied.

(e) Call information Interceptions Using a Pen Register or Trap-and-Trace Device with a Court Order

- (i) Any court order presented by a LEA for call information interception using a pen register or trap-and-trace device shall be referred immediately to the DE.
- (ii) Before authorizing implementation of the interception, the DE shall determine that the court order contains the following information:
 - (1) the identity, if known, of the person to whom the telephone number is assigned or in whose name the telephone number to which the pen register or trap-and-trace device is to be attached;
 - (2) the identity, if known, of the person who is the subject of the criminal investigation;
 - (3) the number and, if known, physical location of the appropriate Multiple Telephone Switching Office to which the pen register or trap-and-trace device is to be attached and, in the case of a trap-and-trace device, the geographical limits of the trap-and-trace order;
 - (4) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates; AND
 - (5) the signature of a judge or magistrate.
- (iii) The DE shall determine whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable Blue Sky to comply with its terms.
- (iv) Once the DE authorizes the implementation of the surveillance and the DE may delegate tasks associated with the surveillance to other employees, but the DE shall continue to oversee the implementation of the surveillance.
- (v) The DE shall complete Blue Sky's Certification Form as soon as possible after the initiation of the electronic surveillance. The DE shall supply all information requested on Blue Sky's Certification Form that is not contained in the court order. The DE then shall attach the court order and sign Blue Sky's Certification Form. The DE also shall attach any extensions that are granted for the surveillance
- (vi) The DE shall make sure that Blue Sky's Certification Form and all attachments are given to the CEO for appropriate filing.

- (vii) The DE shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The DE shall terminate the surveillance at the time specified in the order (which, in the absence of an extension, cannot exceed 60 days).

(f) Call Information Interceptions Using a Pen Register or Trap-and Trace Device without a Court Order

- (i) Requests for call information interception using a pen register or trap-and trace device without a Court Order shall be limited to those instances where it is reasonably determined by a law enforcement officer specially designated by the Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, and Associate Attorney General, any acting Assistant Attorney General, any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any US Territory, State or subdivision thereof, that:
 - (1) an emergency situation exists that involves:
 - (a) immediate danger of death or serious bodily injury to any person; or
 - (b) conspiratorial activities characteristic of organized crime; and
 - (2) there are grounds upon which a Court Order could be entered;
 - (3) Any requests for a call information interception using a pen register or trap-and- trace device without a court order shall be referred immediately to the DE.
 - (4) Although the federal statute does not expressly require a court order in these circumstances, the DE shall make sure that the LEA provides a Certification containing the following information before implementing the request:
 - (a) the information, facilities, or technical assistance required;
 - (b) the period of time during which the provision of information, facilities, or technical assistance is authorized
 - (c) a statement that no warrant or court order is required by law;

- (d) a statement that all statutory requirements have been met; including, but not limited to, a certification that the signatory is duly authorized;
 - (e) a statement that the specific requested assistance is required; AND
 - (f) the signature of a law enforcement officer specially designated by the Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, and Deputy Assistant Attorney General, or by the principal prosecuting attorney of any US Territory, State or subdivision thereof.
- (5) The DE also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.
 - (6) The DE may authorize the implementation of the surveillance and may delegate tasks associated with the surveillance to other employees, but the DE shall continue to oversee the implementation of the surveillance.
 - (7) The DE shall complete Blue Sky's Certification Form as soon as possible after the initiation of the electronic surveillance.
 - (8) The DE shall supply all information requested on Blue Sky's Certification Form that is contained in the LEA Certification.
 - (9) The DE then shall attach the LEA Certification provided and sign Blue Sky's Certification Form.
 - (10) The DE shall make sure that Blue Sky's Certification Form and all attachments are given to the CEO for appropriate filing.
 - (11) The DE shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance as soon as any of the following events occur:
 - (a) the information sought is obtained;
 - (b) the LEA's application for the court order is denied; or
 - (c) 48 hours have lapsed since the installation of the device without the granting of a court order.

- (12) If the LEA does not subsequently receive a Court Order for the surveillance, the DE shall, review the Court Order, and if the DE finds it constitutes appropriate legal authorization, validate the Court Order, attach the Court Order to the Certification Form, and handle the surveillance in all respects.

(g) Electronic Surveillance with a Foreign Intelligence Surveillance Act (“FISA”) Court Order

- (i) Any court order presented to a LEA for electronic surveillance pursuant to FISA shall be referred immediately to the DE.
- (ii) Before implementing the interception, the DE shall make sure that the court order contains the following information:
 - (1) the identity, if known, or a description of the target of the electronic surveillance;
 - (2) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;
 - (3) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
 - (4) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
 - (5) the period of time during which the electronic surveillance is approved;
 - (6) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device;
 - (7) a statement directing that the minimization procedures be followed;
 - (8) a statement directing that, upon the request of the applicant, Blue Sky shall furnish the applicant with all information, facilities, or 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 Blue Sky is providing that target of electronic surveillance;

- (9) a statement directing that Blue Sky maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance; AND
 - (10) the signature of a federal district judge.
- (h) **Whenever the target of the electronic surveillance is a foreign power (as defined under FISA) and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the court order need not contain the information required by subparagraphs (c), (d), and (f), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.**
- (i) The DE also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately detailed to enable, Blue Sky to comply with its terms.
 - (ii) The DE may authorize the implementation of the surveillance and may delegate Tasks associated with the surveillance to other employees, but the DE shall continue to oversee the implementation of the surveillance.
 - (iii) The DE shall complete Blue Sky's Certification Form as soon as possible after the initiation of the electronic surveillance. The DE shall supply any information requested on Blue Sky's Certification Form that is not contained in the court order. The DE then shall attach the court order and sign Blue Sky's Certification Form. The DE also shall attach any extensions that are granted for the surveillance.
 - (iv) The DE shall make sure that Blue Sky's Certification Form and all attachments are given to the CEO for appropriate filing.
 - (v) The DE continues to oversee the conduct of the electronic surveillance and make sure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the order. In the absence of an extension, the surveillance cannot exceed 90 days (or 1 year if the surveillance is targeted against a foreign power).
- (i) **Electronic Surveillance Conducted Pursuant to FISA without a Court Order**
- (i) Any requests by a LEA for electronic surveillance pursuant to FISA but without a court order shall be referred immediately to the DE.

- (ii) Although the FISA does not expressly require a certification in these circumstances, the designated employee shall make sure that the LEA provides a certification containing the following information before authorizing implementation of the request:
- (1) the information, facilities, or technical assistance required;
 - (2) the period of time during which the provision of information, facilities, or technical assistance is authorized;
 - (3) a statement that no warrant or court order is required by law;
 - (4) a statement that all statutory requirements have been met, including, but not limited to, a certification that the signatory is duly authorized;
 - (5) a statement that the specific requested assistance is required; AND
 - (6) the signature of either
 - (a) the Attorney General of the United States, OR
 - (b) a law enforcement officer specially designated by the Attorney General
 - (7) The DE also shall determine whether the surveillance can be implemented technically AND whether the LEA Certification is sufficiently and accurately detailed to enable Blue Sky to comply with its terms.
 - (8) The DE may authorize the implementation of the surveillance and may delegate tasks associated with the surveillance to other employees, but the DE shall continue to oversee the implementation of the surveillance.
 - (9) The DE shall complete Blue Sky's Certification Form as soon as possible after the initiation of the electronic surveillance. The DE shall supply all information requested on Blue Sky's Certification Form that is not contained in the LEA Certification. The DE then shall attach the LEA Certification Form and sign Blue Sky's Certification Form.
 - (10) The DE shall make sure that Blue Sky's Certification Form and all attachments are placed in the appropriate file.
 - (11) The DE shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance as soon as any of the following events occur:

- (a) the information sought is obtained;
- (b) the LEA's application for a Court Order is denied; or
- (c) 24 hours have elapsed since the authorization of the surveillance by the Attorney General without the granting of a Court Order.

(12) If the LEA does subsequently receive a Court Order for the surveillance, the DE shall review the Court Order, and if the DE finds it constitutes appropriate legal authorization, validate the Court Order, attach the Court Order to the Certification Form, and handle the surveillance in all respects.

(j) Procedures if Unauthorized Surveillance or a Compromise of Surveillance has Occurred

- (i) If any employee becomes aware of any act of unauthorized electronic surveillance that occurred on Blue Sky's premises or any compromise of authorized surveillance to unauthorized persons or entities, that employee shall report the incident immediately to the DE.
- (ii) The DE shall promptly notify legal counsel of the incident. Acting with legal counsel, the DE and legal counsel shall determine which LEAs are affected and promptly notify the agencies of the incident. The DE shall compile a certification record in Exhibit 2 for any unauthorized surveillance and make sure that all records available to Blue Sky regarding the surveillance are given to the CEO for appropriate filing.

EXHIBIT 1

Blue Sky Certification Form Certification Form for Electronic Surveillance Implemented by Blue Sky

INSTRUCTIONS: Fill in all information. If court order is used in lieu of providing information, attach copy of court order and any extension granted.

TODAY'S DATE: _____

TELEPHONE NUMBER(S) AND/OR CIRCUIT IDENTIFICATION NUMBERS INVOLVED:

START DATE AND TIME OF THE OPENING OF THE CIRCUIT FOR LAW ENFORCEMENT: _____

IDENTITY OF LAW ENFORCEMENT PERSONNEL PRESENTING THE AUTHORIZATION: _____

NAME OF CALEA CONTACT OFFICER OVERSEEING ACTION:

TYPE OF INTERCEPTION OR ACCESS TO CALL-IDENTIFYING INFORMATION (e.g., pen register, trap and trace, Title III, FISA): _____

CALEA CONTACT OFFICER OVERSEEING INTERCEPTION OR ACCESS:

CERTIFICATION

I, _____, am a CALEA Contact Officer, listed in Appendix A. [Employees Designated as CALEA Contact Officers], I have overseen the electronic surveillance described on this form and on any attached documents, and I hereby certify that to the best of my knowledge and belief, the information contained on this form and the attached documents is complete and accurate.

Signed: _____

Date: _____

Title: _____

CALEA INCIDENT REPORT

The following incident occurred involving (circle one) an act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities / an act of unlawful electronic surveillance that occurred on the carrier's premises:

CALEA Contact Officer TITLE DATE

APPENDIX A

CALEA CONTACT OFFICER(S)

CONTACT INFORMATION AND JOB DESCRIPTION

CALEA Contact Officer:

Name: Adolfo Montenegro
Title: Chief Executive Officer
Phone Numbers: 684-699-2759 (during business hours)
684-258-1016 (after hours/emergency 24/7)

Name: Alex Alan Ramirez
Title: Director of Engineering and Operations
Phone Numbers: 684-699-2759 (during business hours)
684-258-1002 (after hours/emergency 24/7)

Name: Li'a Tufele, Jr.
Title: Chief Technology Officer
Phone Numbers: 684-699-2759 (during business hours)
684-258-1072 (after hours/emergency 24/7)

Job Descriptions:

The Chief Executive Officer, Director of Engineering and Operations and the Chief Technology Officer are all responsible for CALEA compliance. Each will serve as a Designated Employee (DE) or CALEA Contact Officer for Company.