



RECEIVED

JUL - 2 2001

FCC MAIL ROOM

July 2, 2001

Federal Communications Commission
Office of the Secretary
445 12th Street, S.W.
12th Street Lobby, TW-A325
Washington, DC 20554

ATTENTION: COMMON CARRIER BUREAU

Dear Secretary:

Frontier Communications is filing the Communications Assistance for Law Enforcement Act (CALEA) Security Compliance Manual. This filing is in compliance with CC Docket 97-213.

Frontier Communications is currently included in the Global Crossing North America, Inc. CALEA Security Compliance Manual filed with the Common Carrier Bureau on May 1, 2000.

On June 30, 2001, Global Crossing North America, Inc. sold the Frontier Communications companies to the Citizens Communications Company. Therefore, Frontier Communications is filing a revised CALEA Security Compliance Manual separate from Global Crossing North America, Inc.

Please initial and return a copy of this letter in the return addressed envelope provided to acknowledge receipt.

If you have any questions, please contact Cassandra Guinness at 716-777-4557 or e-mail cassandra_guinness@frontiercorp.com.

Sincerely,

Cassandra Guinness
Cassandra Guinness
Sr. Regulatory Analyst

No. of Copies rec'd _____
List ABCDE _____

0

Frontier Communications

Corporate Security Services (CSS)

Communications Assistance for Law Enforcement Act (CALEA)

Compliance Manual

Adopted: 7-1-2001

Filed with the Federal Communications Commission: 7-2-2001

TABLE OF CONTENTS

I.	CORPORATE POLICY STATEMENT	1
II.	DEFINITIONS	4
III.	GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE.	4
	A. "Appropriate Authorization" Required To Conduct Electronic Surveillance.	4
	B. Employees Designated as Points of Contact	4
	C. Duties of Designated Employees.	5
	D. Recordkeeping.	6
	E. Unauthorized Surveillance and Compromises of Authorized Surveillance	7
IV.	PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE	7
	A. Call Content Interceptions with a Title III Court Order	7
	B. Call Content Interceptions Pursuant to Title III but without a Court Order	8
	C. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device with a Court Order	9
	D. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device without a Court Order	10
	E. Electronic Surveillance with a Foreign Intelligence Surveillance Act ("FISA") Court Order	11
	F. Electronic Surveillance Conducted Pursuant to FISA but without a Court Order	12
V.	PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED	14

APPENDICES

APPENDIX I - Cover Sheet and Certification Form for Electronic Surveillance Implemented By:

Frontier Communications

APPENDIX 2 - Example of a Court Order Submitted by a Law Enforcement Agency for a Call Information Interception

APPENDIX 3 - Relevant Federal Statutes

18 U.S.C. §§ 2510-2522 (Title III interceptions)

18 U.S.C. §§ 3121-3217 (Pen Register and Trap-and-Trace Surveillance)

50 U.S.C. §§ 1801-1811 (Foreign Intelligence Surveillance Act)

I. STATEMENT OF CORPORATE POLICY

It is the policy of **Frontier Communications** to comply with the 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 constitutes the required policies and procedures for **Frontier Communications' ILECs, IXCs and CLECs** listed below:

Incumbent Local Exchange Carriers (ILEC):

Frontier Telephone of Rochester
Frontier Communications of Alabama, Inc.
Frontier Communications of the south, Inc
Frontier Communications of Lamar County, Inc.
Frontier Communications of Depue, Inc.
Frontier Communications of Illinois, Inc.
Frontier Communications of Lakeside, Inc.
Frontier Communications of Midland, Inc.
Frontier Communications of Mt. Pulaski, Inc.
Frontier Communications of Orion, Inc.
Frontier Communications of Prairie, Inc.
Frontier Communications of Schulyer, Inc.
Frontier Communications of Georgia, inc.
Frontier Communications of Iowa, Inc.
Frontier Communications of Indiana, Inc.
Frontier Communications of Thorntown, Inc.
Frontier Communications of Mississippi, Inc.
Frontier Communications of Michigan, Inc.
Frontier Communications of Minnesota, Inc.
Frontier Communications of Ausable Valley, Inc.
Frontier Communications of New York, Inc.
Frontier Communications of Seneca Gorham, Inc.
Frontier Communications of Sylvan Lake
Frontier Communications of Breezewood, Inc.
Frontier Communications of Canton, Inc.
Frontier Communications of Oswayo River, Inc.
Frontier Communications of Pennsylvania
Frontier Communications of Wisconsin, Inc.
Frontier Communications of Viroqua, Inc.
Frontier Communications of Mondovi, Inc.

Interexchange Carriers (IXC)

Frontier Communications of America, Inc.

Competitive Local Exchange Carriers (CLEC)

Frontier Communications of Rochester, Inc.

All employees are required to follow the policies and procedures specified in this 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: **William Barnes**, **Corporate Security Services, (716) 777-5179.**
- ❑ Any violation of or departure from the policies and procedures in this Manual should be reported immediately to: **William Barnes**, **Corporate Security Services, (716) 777-5179.**

II. DEFINITIONS (AS THEY APPEAR IN THIS DOCUMENT)

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

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

Carrier - a person engaged in the transmission or switching of wire or electronic communications as a common carrier for hire (including commercial mobile service) except insofar as the person is engaged in providing information services

Electronic surveillance - the implementation of either a call content interception or a call information interception.

Title III (Eavesdropping Warrant) - Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which is the federal statute that sets minimum legal requirements for all call content interceptions by government officials and private citizens (except for those interceptions authorized under the Foreign Intelligence Surveillance Act). Title III is codified at 18 U.S.C. §§ 2510-2520.

III. GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE

A. "Appropriate Authorization" Required To Conduct Electronic Surveillance

It is the policy of **Frontier Communications** to permit only lawful, authorized electronic surveillance to be conducted on its premises.

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. Section IV of this Compliance Manual sets forth how each form of authorization is to be obtained.

B. Employees Designated as Points of Contact

Frontier Communications hereby designates the following employees to serve as points of contact for law enforcement agencies. The employees shall be available to law enforcement agencies during the times listed below, so that law enforcement agencies will always be able to contact at least one employee 24 hours a day, 7 days a week. If an employee cannot be available at a designated time, that employee shall arrange for one of other employees listed below to be available during that time.

- | | | |
|--|-------------|--|
| 1. <u>William J. Barnes</u>
Corporate Security Services | 24hrs/7days | ofc > 716-777-5179
pager > 716-246-4899
cell > 716-721-1140
24hr # > 716-777-7773 |
| 2. <u>Mary M. Delaney</u>
Corporate Security Services | 24hrs/7days | ofc > 716-777-6859
pager > 716-955-2520
cell > 716-329-4854
24hr # > 716-777-7773 |
| 3. <u>John D. Heaney</u>
Corporate Security Services | 24hrs/7days | ofc > 716-777-8816
pager > 716-327-8394
cell > 716-329-4687
24hr # > 716-777-7773 |
| 4. <u>Mary Jo Evans</u>
Corporate Security Services | 24hrs/7days | ofc > 716-777-5079
cell > 716-233-2171
24hr # > 716-777-7773 |

C. Duties and Responsibilities of Designated Employees

1. The employees designated in Section **III.B** above are hereby authorized by **Frontier Communications** to implement lawful electronic surveillance in accordance with the policies and procedures in this Manual and to delegate any tasks associated with the surveillance to other employees.

2. An employee designated in Section **III.B** above shall:

- Oversee the implementation of each electronic surveillance conducted on the premises of **Frontier Communications**
- Be 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:
 - (i) immediate danger of death or serious physical injury to any person,
 - (ii) conspiratorial activities threatening the national security interest, or
 - (iii) conspiratorial activities characteristic of organized crime.

NOTE: The relevant federal statutory provisions are attached as Appendix 3, and procedures for compliance with them are set forth in Section IV of this Manual. The relevant state statutory provisions are attached as Appendix 4.)

- Affirmatively intervene to ensure that there is appropriate legal authorization for each electronic surveillance, including any appropriate authorization required under relevant state and federal statutes;
- Complete a certification form for each electronic surveillance he/she oversees and do so within **24 hours** of the initiation of, the surveillance.
- Ensure that all records, for each surveillance, are placed in the appropriate file.

3. **Frontier Communications Corporate Security Services** shall ensure that this document is updated and filed with the FCC within **90** days of any amendment or Frontier Communications merger with another company.

D. Recordkeeping

The designated employee shall complete a certification form (Appendix 1) for *every* electronic surveillance conducted on company premise - regardless of whether the surveillance was authorized or unauthorized.

Frontier Communications shall establish and label separate files in which it will retain all certification, forms, court orders, and other records for (1) **authorized call content interceptions;** (2) **unauthorized call content interceptions;** and (3) **authorized and unauthorized call information interceptions.** These records shall be retained in secure and appropriately marked files for a **period of seven (7) years** from the time the **termination of the surveillance.** It has been the custom and policy of **Frontier Communications** to maintain these records for this period of time, and experience has shown that this policy has adequately served the needs of Frontier Communications and law enforcement agencies.

E. Unauthorized Surveillance and Compromises of Authorized Surveillance

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 may be appropriate.

Employees shall report any incidents of unauthorized surveillance and any compromises of authorized surveillance in accordance with the procedures in Section V of this Manual.

IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE

A. Call Content Interceptions with a Title III Court Order

Step One. Any court order presented by a law enforcement agency for a call content interception, pursuant to Title III, shall be referred immediately to one of the employees designated in Section **III.B** of this Manual.

Step Two. Before implementing the interception, the designated employee shall ensure that the court order contains the following information:

- (a) the identity of the person, if known, whose communications are to be intercepted;
- (b) the nature and location of the communications facilities or the place for which authority to intercept is granted
- (c) a particular description of the type of communication sought to be intercepted and a of the particular offense to which it relates;
- (d) 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;
- (e) 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 subject to interception; and
- (f) the signature of a judge or magistrate.

- Step Three. The designated employee also shall determine whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable compliance with its terms
- Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.
- Step Five. The designated employee shall complete and **sign**, a Certification Form (Appendix 1) within 24 hours of the initiation of the electronic surveillance. The employee shall attach the Certification Form to the court order. All extensions, granted for the surveillance, are to be attached to the Certification Form
- Step Six. The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the court order.

B. Call Content Interceptions, Pursuant to Title III, but *without* a Court Order

- Step One. Any request by a law enforcement agency 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 one of the employees designated in Section **III.B** of this Manual.
- Step Two. Before implementing the interception, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information:
- (a) the information, facilities, or technical assistance required;
 - (b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
 - (c) a statement that no warrant or court order is required by law;
 - (d) a statement that all statutory requirements have been met;
 - (e) a statement that the specific requested assistance is required; AND
 - (f) the signature of **EITHER** (i) the Attorney General of the United States, OR (ii) a law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

- Step Three. The designated employee also shall determine whether the surveillance can be implemented technically and whether the certification is sufficiently and accurately detailed to enable compliance with its terms.
- Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.
- Step Five. The designated employee shall complete and **sign**, a Certification Form (Appendix 1) within 24 hours of the initiation of the electronic surveillance. The employee shall attached that Certification Form to the certification provided by the law enforcement agency.
- Step Six. The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven. The designated employee 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 law enforcement agency does not apply for a court order within 48 hours after the interception has begun; or
 - (b) the law enforcement agency's application for a court order is denied.
- Step Eight. If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.A, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section IV.A.

C. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device with a Court Order

- Step One. Any court order presented by a law enforcement agency for a call information interception using -a pen register or trap-and-trace device shall be referred immediately to one of the employees designated in Section III.B of this M
- Step Two. Before implementing the interception, the designated employee shall determine that the court order contains the following information:
- (a) the identity, if known, 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;
 - (b) the identity, if known, of the person who is the subject of the criminal investigation;
 - (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 and, in the case of a trap and-trace device, the geographical limits of the trap-and-trace order;

(d) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates; AND

(e) the signature of a judge or magistrate.

[A sample court order for a pen register or trap-and-trace device is attached as Appendix 2.]

- Step Three. The designated employee also shall determine whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable compliance with its terms.
- Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.
- Step Five. The designated employee shall complete and **sign**, a Certification Form (Appendix 1) within 24 hours of the initiation of the electronic surveillance. The employee shall attached the Certification Form to the court order. All extensions, granted for the surveillance, are to be attached to the Certification Form
- Step Six. The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The designated employee shall terminate the surveillance at the time specified in the order. In the absence of an extension, the surveillance can not exceed 90 days. (One (1) year if surveillance is targeted against a foreign power)

D. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device *without* a Court Order

- Step One. Any request for a call information interception using a pen register or trap-and trace device without a court order shall be referred immediately to one of the employees designated in Section III of this Manual.
- Step Two. Although the federal statute does not expressly require a certification in these circumstances, the designated employee shall ensure that the law enforcement agency 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;
 - (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, any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof

- Step Three. The designated employee also shall determine whether the surveillance can be implemented technically and whether the certification is sufficiently and accurately detailed to enable compliance with its terms.
- Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.
- Step Five. The designated employee shall complete and **sign**, a Certification Form (Appendix 1) within 24 hours of the initiation of the electronic surveillance. The employee shall attach the Certification Form to the certification provided by the law enforcement agency.
- Step Six. The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven. The designated employee 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 law enforcement agency'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
- Step Eight. If the law enforcement agency **does** receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.C, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section IV.C.

E. Electronic Surveillance with a Foreign Intelligence Surveillance Act ("FISA") Court Order

- Step One. Any court order presented by a law enforcement agency for electronic surveillance pursuant to FISA shall be referred immediately to one of the employees designated in Section III.B of this Manual.
- Step Two. Before implementing the interception, the designated employee shall ensure that the court order contains the following information:
- (a) the identity, if known, or a description of the target of the electronic surveillance;
 - (b) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

- (c) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
- (d) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
- (e) the period of time during which the electronic surveillance is approved;
- (f) 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;
- (g) a statement directing that the minimization procedures be followed;
- (h) a statement directing that, upon the request of the applicant, a specified carrier furnish the applicant forthwith 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 the carrier is providing that target of electronic surveillance;
- (i) a statement directing that the carrier maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain;
- (j) statement directing that the applicant compensate, at the prevailing rate, the carrier for furnishing the aid; AND
- (k) the signature of a federal district judge.

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.

- Step Three. The designated employee also shall determine whether the surveillance can be implemented technically and whether the court order is sufficiently and accurately detailed to enable compliance with its terms.
- Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.
- Step Five. The designated employee shall complete and **sign**, a Certification Form (Appendix 1) within 24 hours of the initiation of the electronic surveillance. The employee shall attached the Certification Form to the court order. All extensions, granted for the surveillance, are to be attached to the Certification Form

- Step Six. The designated employee shall ensure that the Certification Form and all
- Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the order.

F. Electronic Surveillance Conducted Pursuant to FISA but *without* a Court Order

- Step One. Any request by a law enforcement agency for electronic surveillance pursuant to FISA but without a court order shall be referred immediately to one of the employees designated in Section **III.B** of this Manual.
- Step Two. Although FISA does not expressly require a certification in these circumstances, the designated employee shall ensure that the law enforcement agency 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;
 - (e) a statement that the specific requested assistance is required; **AND**
 - (f) the signature of **EITHER** (i) the Attorney General of the United States, **OR** (ii) a law enforcement officer specially designated by the Attorney General.
- Step Three. The designated employee also shall determine whether the surveillance can be implemented technically and whether the certification is sufficiently and accurately detailed to enable compliance with its tenants.
- Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.
- Step Five. The designated employee shall complete and **sign**, a Certification Form (Appendix 1) within 24 hours of the initiation of the electronic surveillance. The employee shall attached the Certification Form to the certification provided by the law enforcement agency
- Step Six. The designated employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven. The designated employee 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 law enforcement agency'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.

Step Eight. If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.E, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section W.E.

V. **PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED**

Step One. If any employee becomes aware of any act of unauthorized electronic surveillance or any compromise of authorized surveillance to unauthorized persons or entities, that employee shall report the incident immediately to one of the employees designated in Section III.B of this Manual.

Step Two. The designated employee shall promptly notify **Corporate Security Services** of the incident. Acting with **legal counsel**, the **designated employee** and **Corporate Security Services** shall determine which law enforcement agencies are affected and promptly notify the agencies of the incident.

Step Three. The designated employee shall compile a certification record for any unauthorized surveillance and ensure that all records available to the carrier, regarding the surveillance, are placed in the appropriate files.

APPENDIX 1

Certification Form for Electronic Surveillance

Frontier Communications

CORPORATE SECURITY SERVICES PEN REGISTER AND WIRE TAP DATA CERTIFICATION COVER SHEET

TYPE OF ORDER: (Check)

Pen Register ___ Title III ___ Trap & Trace ___ FISA ___

TARGET TELEPHONE #: () _____

Len: _____

Class of Service: _____

Date: Installed: _____ Date Removed: _____

Subscriber Name: _____

Address: _____

TRUNK ASSIGNMENT/LOCATION FOR REMOTE DNR

_____ CABLE PAIR _____

_____ CABLE PAIR _____

_____ CABLE PAIR _____

DIAL-UP #: _____

LEN: _____

Agency & Billing address: _____ Circuit Order #: _____

Frontier Communications

Certification Form for Electronic Surveillance:

INSTRUCTIONS: The information requested below shall be provided either on this form or by attaching the appropriate legal authorization for the surveillance if the authorization contains that information. If the authorization is attached, check the box below and attach any extensions that are granted for the surveillance.

I have attached the court order or other legal authorization for this surveillance as well as any extensions that have been granted.

1. Telephone number(s) and/or circuit Identification numbers involved	
2. Start date and time of the opening of the circuit for law enforcement	
3. Law enforcement officer presenting the Authorization	
4. Person signing the appropriate legal Authorization	
5. Type of surveillance (e.g., pen register, trap and trace, Title III , FISA)	
6. Designated employee responsible for Overseeing the surveillance	

I, _____, have overseen the electronic surveillance described on this form and on any attached documents, and I hereby certify that the information contained on this form is complete and accurate.

APPENDIX 2

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

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, Sections 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 [Carrier] 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

IT IS FURTHER ORDERED, that [Carrier] be compensated by the applicant for reasonable expenses incurred in providing technical assistance; and

IT IS FURTHER ORDERED, that [Carrier] shall supply (**Investigative Agency**) with subscriber information, including published and nonpublished telephone information, for those telephone numbers, names or addresses identified in this order and/or obtained by the pen register and/or trap 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 [Carrier], 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 basis 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 carrier cannot provide information that is not specified and required by court order. Title III Wire Intercepts follow the same basic format; however, the time frame cannot exceed 30 days.

APPENDIX 3

Relevant Federal Statutes:

18 U.S.C. §§ 2510-2522 (Title III interceptions)

18 U.S.C. §§ 3121-3217 (Pen Register and Trap-and-Trace Surveillance)

50 U.S.C. §§ 1801-1811 (Foreign Intelligence Surveillance Act)

APPENDIX 3

Relevant Federal Statutes

TITLE 18. CRIMES AND CRIMINAL PROCEDURE

PART I—CRIMES

CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Section 2510. Definitions

As used in this chapter—

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

- (A) any wire or oral communication;
- (B) any communication made through a tone-only paging device;
- (C) any communication from a tracking device (as defined in section 3117 of this title); or
- (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who--

- (A) uses an electronic communication service; and
- (B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--

- (A) scrambled or encrypted;
- (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
- (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
- (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
- (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

[(F) Repealed. Pub.L. 104-132, Title VII, S 731(2)(C), Apr. 24, 1996, 110 Stat. 1303]

(17) "electronic storage" means--

- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
- (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

Section 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who--

- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
- (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--
 - (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
 - (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
 - (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

- (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
- (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;
- (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
- (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
- (e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b) to (c), 2511(2)(e), 2516, and 2518 of this chapter,
 - (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,
 - (iii) having obtained or received the information in connection with a criminal investigation, and
 - (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,
 shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).
- (2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
 - (ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--
 - (A) a court order directing such assistance signed by the authorizing judge, or
 - (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,
 setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.
- (b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept

a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(3) (a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other

than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

- (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;
- (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
- (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
- (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4) (a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then--

- (i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and
- (ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

- (i) to a broadcasting station for purposes of retransmission to the general public; or
- (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5) (a) (i) If the communication is--

- (A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or
- (B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

- (A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and
- (B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

Section 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

- (1) Except as otherwise specifically provided in this chapter, any person who intentionally--
- (a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;
 - (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or
 - (c) places in any newspaper, magazine, handbill, or other publication any advertisement of--
 - (i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
 - (ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

- (2) It shall not be unlawful under this section for--
- (a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or
 - (b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

Section 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person

with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

Section 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

Section 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of--

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots) chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146

(relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), and section 1341 (relating to mail fraud), section 351 (violations) with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline) or section 46502 (relating to aircraft piracy) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens);

(p) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the

offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

Section 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

Section 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of

interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and
(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain 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 under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the

intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

- (i) immediate danger of death or serious physical injury to any person,
- (ii) conspiratorial activities threatening the national security interest, or
- (iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

- (1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if--

(a) in the case of an application with respect to the interception of an oral communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

(iii) the judge finds that such purpose has been adequately shown.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (1)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

Section 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts--

- (a) the fact that an order or extension was applied for;
- (b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);
- (c) the fact that the order or extension was granted as applied for, was modified, or was denied;
- (d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- (e) the offense specified in the order or application, or extension of an order;
- (f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and
- (g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts--

- (a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;
- (b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;
- (c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;
- (d) the number of trials resulting from such interceptions;
- (e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;
- (f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and
- (g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding

regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

Section 2520. Recovery of civil damages authorized

(a) **In general.**--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) **Relief.**--In an action under this section, appropriate relief includes--

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c) and punitive damages in appropriate cases; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) **Computation of damages.**--

(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$50 and not more than \$500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of--

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

(d) **Defense.**--A good faith reliance on--

- (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
- (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
- (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) **Limitation.**--A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

Section 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

Section 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by court issuing surveillance order.--If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement upon application by Attorney General.--The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil penalty.--

(1) In general.--A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to \$10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) Considerations.--In determining whether to impose a civil penalty and in determining its amount, the court shall take into account--

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(C) such other matters as justice may require.

(d) Definitions.--As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

**TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II—CRIMINAL PROCEDURE
CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES**

Section 3121. General prohibition on pen register and trap and trace device use; exception

- (a) *In general.*--Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).
- (b) *Exception.*--The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--
- (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
 - (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
 - (3) where the consent of the user of that service has been obtained.
- (c) *Limitation.*--A government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.
- (d) *Penalty.*--Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

Section 3122. Application for an order for a pen register or a trap and trace device

- (a) *Application.*--
- (1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.
 - (2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.
- (b) *Contents of application.*--An application under subsection (a) of this section shall include--
- (1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
 - (2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Section 3123. Issuance of an order for a pen register or a trap and trace device

- (a) *In general.*--Upon an application made under section 3122 of this title, the court shall enter an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
- (b) *Contents of order.*--An order issued under this section--
- (1) shall specify--

- (A) the identity, if known, 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;
 - (B) the identity, if known, of the person who is the subject of the criminal investigation;
 - (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 and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and
 - (D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
- (2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.
- (c) Time period and extensions.--
- (1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.
 - (2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.
- (d) Nondisclosure of existence of pen register or a trap and trace device.--An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--
- (1) the order be sealed until otherwise ordered by the court; and
 - (2) the person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, 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 or until otherwise ordered by the court.

Section 3124. Assistance in installation and use of a pen register or a trap and trace device

- (a) Pen registers.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.
- (b) Trap and trace device.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.
- (c) Compensation.--A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.
- (d) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or

other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this chapter or request pursuant to section 3125 of this title.

(e) Defense.—A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications assistance enforcement orders.—Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

Section 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines 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,

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

Section 3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice.

Section 3127. Definitions for chapter

As used in this chapter—

(1) the terms "wire communication", "electronic communication", and "electronic communication service" have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means—

(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

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

(4) the term "trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

**TITLE 50. WAR AND NATIONAL DEFENSE
CHAPTER 36--FOREIGN INTELLIGENCE SURVEILLANCE
SUBCHAPTER I--ELECTRONIC SURVEILLANCE**

Section 1801. Definitions

As used in this subchapter:

- (a) "Foreign power" means--
- (1) a foreign government or any component thereof, whether or not recognized by the United States;
 - (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
 - (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
 - (4) a group engaged in international terrorism or activities in preparation therefor;
 - (5) a foreign-based political organization, not substantially composed of United States persons; or
 - (6) an entity that is directed and controlled by a foreign government or governments.
- (b) "Agent of a foreign power" means--
- (1) any person other than a United States person, who--
 - (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
 - (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
 - (2) any person who--
 - (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
 - (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
 - (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or
 - (D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).
- (c) "International terrorism" means activities that--
- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
 - (2) appear to be intended--
 - (A) to intimidate or coerce a civilian population;
 - (B) to influence the policy of a government by intimidation or coercion; or
 - (C) to affect the conduct of a government by assassination or kidnapping; and
 - (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
- (d) "Sabotage" means activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States.
- (e) "Foreign intelligence information" means--
- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
- (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--
 - (A) the national defense or the security of the United States; or
 - (B) the conduct of the foreign affairs of the United States.
- (f) "Electronic surveillance" means--
 - (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
 - (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;
 - (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
 - (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.
- (g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.
- (h) "Minimization procedures", with respect to electronic surveillance, means--
 - (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
 - (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
 - (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
 - (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.
- (i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.
- (j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

Section 1802. Electronic surveillance authorization without court order; certification by Attorney General; reports to Congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction of court

(a) (1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that--

(A) the electronic surveillance is solely directed at--

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808(a) of this title.

(3) The Attorney General shall immediately transmit under seal to the court established under section 1803(a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless--

(A) an application for a court order with respect to the surveillance is made under sections 1801(h)(4) and 1804 of this title; or

(B) the certification is necessary to determine the legality of the surveillance under section 1806(f) of this title.

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to--

(A) furnish 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 such carrier is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order under this subchapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

Section 1803. Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review

The Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b) of this section.

(b) Court of review; record, transmittal to Supreme Court

The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) Expeditious conduct of proceedings; security measures for maintenance of records

Proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

(d) Tenure

Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated

for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years.

Section 1804. Applications for court orders

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include--

- (1) the identity of the Federal officer making the application;
- (2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
- (3) the identity, if known, or a description of the target of the electronic surveillance;
- (4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that--
 - (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
 - (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (5) a statement of the proposed minimization procedures;
- (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
- (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate--
 - (A) that the certifying official deems the information sought to be foreign intelligence information;
 - (B) that the purpose of the surveillance is to obtain foreign intelligence information;
 - (C) that such information cannot reasonably be obtained by normal investigative techniques;
 - (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
 - (E) including a statement of the basis for the certification that--
 - (i) the information sought is the type of foreign intelligence information designated; and
 - (ii) such information cannot reasonably be obtained by normal investigative techniques;
- (8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;
- (9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;
- (10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and
- (11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

(b) Exclusion of certain information respecting foreign power targets

Whenever the target of the electronic surveillance is a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), and (11) of subsection (a) of this section, but shall state whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

(c) Additional affidavits or certifications

The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(d) Additional information

The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title.

Section 1805. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--

- (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
- (2) the application has been made by a Federal officer and approved by the Attorney General;
- (3) on the basis of the facts submitted by the applicant there is probable cause to believe that--
 - (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
 - (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
- (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

(b) Specifications and directions of orders

An order approving an electronic surveillance under this section shall--

- (1) specify--
 - (A) the identify, if known, or a description of the target of the electronic surveillance;
 - (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;
 - (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

- (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
- (E) the period of time during which the electronic surveillance is approved; and
- (F) 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; and

(2) direct--

- (A) that the minimization procedures be followed;
- (B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith 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 such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;
- (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
- (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(c) Exclusion of certain information respecting foreign power targets

Whenever the target of the electronic surveillance is a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (b)(1) of this section, 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.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

- (1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less.
- (2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period.
- (3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Emergency orders

Notwithstanding any other provision of this subchapter, when the Attorney General reasonably determines that--

- (1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and
- (2) the factual basis for issuance of an order under this subchapter to approve such surveillance exists; he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

(f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel

Notwithstanding any other provision of this subchapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to--

- (1) test the capability of electronic equipment, if--
 - (A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;
 - (B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;
 - (C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and
 - (D) Provided, That the test may exceed ninety days only with the prior approval of the Attorney General;
- (2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if--
 - (A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;
 - (B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and
 - (C) any information acquired by such surveillance is used only to enforce chapter 119 of Title 18, or section 605 of Title 47, or to protect information from unauthorized surveillance; or
- (3) train intelligence personnel in the use of electronic surveillance equipment, if--
 - (A) it is not reasonable to--
 - (i) obtain the consent of the persons incidentally subjected to the surveillance;
 - (ii) train persons in the course of surveillances otherwise authorized by this subchapter; or
 - (iii) train persons in the use of such equipment without engaging in electronic surveillance;

- (B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and
- (C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Retention of certifications, applications and orders

Certifications made by the Attorney General pursuant to section 1802(a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application.

Section 1806. Use of information

(a) Compliance with minimization procedures; privileged communications; lawful purposes

Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

- (1) the information was unlawfully acquired; or
- (2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon

recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

- (1) the fact of the application;
- (2) the period of the surveillance; and
- (3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

Section 1807. Report to Administrative Office of the United States Court and to Congress

In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year--

- (a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and
- (b) the total number of such orders and extensions either granted, modified, or denied.

Section 1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress

(a) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this subchapter. Nothing in this subchapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

Section 1809. Criminal sanctions

(a) Prohibited activities

A person is guilty of an offense if he intentionally--

- (1) engages in electronic surveillance under color of law except as authorized by statute; or

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

(b) Defense

It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) Penalties

An offense described in this section is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.

(d) Federal jurisdiction

There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

Section 1810. Civil liability

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover--

- (a) actual damages, but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater;
- (b) punitive damages; and
- (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

Section 1811. Authorization during time of war

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.