Pennsylvania Chiefs of Police Association

Request For Information

Police Body Worn Cameras

(A.K.A. non-vehicle-mounted mobile video recording systems)

January 8, 2019

The Pennsylvania Chiefs of Police Association (PCPA) in cooperation with the Local Technology Workgroup (LTW) of the Pennsylvania Commission on Crime and Delinquency PCCD) is requesting any information from manufactures, vendors or resellers that would assist Pennsylvania's police departments in purchasing police officer worn body camera.

BACKGROUND

The Pennsylvania Chiefs of Police Association (PCPA) with the Local Technology Workgroup (LTW) of the Pennsylvania Commission on Crime and Delinquency PCCD) has been working with several hundred police departments on purchasing and deploying body worn cameras. PCCD has been awarded over a million dollars in federal grant funds to assist the procurement of police worn body cameras. However, Pennsylvania has specific laws and regulations on the use of non-vehicle-mounted mobile video recording systems and the federal grant has more requirements. Therefore, PCPA on behalf of Pennsylvania's police departments is requesting information from anyone in the business of providing equipment and services as defined by Pennsylvania Law and regulations of non-vehicle-mounted mobile video recording systems.

Pennsylvania has over 30,000 sworn officers working in over 1200 police departments. PCPA believes providing this information to us benefits both the police departments and the providers of these body worn cameras and their accompanying services. While some departments will only require a few body worn cameras and simple storage solutions, others will need hundreds and complex storage. Providing this information to PCPA, LTW, PCCD and Pennsylvania's police departments will allow a more complete understanding of the technology, products and the service they can acquire.

The benefit to manufactures, vendors or resellers is that you get the opportunity to present your technology products and services in a fashion that meets the specific needs of Pennsylvania's police and presents that to a large group leading the state effort.

INFORMATION REQUESTED

The information requested includes the manufactures, vendors or resellers of specific products and services that meet Pennsylvania Laws, standards and regulations that allow them to develop the necessary polices required. In addition, cost and discounted price are requested. Please provide at least the following information:

- How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?
- Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?
- Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?
- Are you offering a storage solution?
- Will you offer storage solutions bundled (no line item distinction)with the cost of each camera purchased?

- How does your storage solution meet Pennsylvania's published requirements?
- List the products and services that are already available on State Contract or PA CoStars.
- List your costs for products and services you offer.
- Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

PENNSYLANIA LAWS AND PUBLISHED REQUIREMENTS

To help you provide your information the following laws and published standards and regulations are in the APPENDIX attached to this RFI:

- PA Title 18 CHAPTER 57 WIRETAPPING AND ELECTRONIC SURVEILLANCE
- PA ACT 22, 2017
- PA Bulletin Doc 45 5482, 8/29/15
- PA Bulletin Doc 45 5712, 9/19/15
- PA Bulletin Doc 46 116, 1/2/16
- PA Bulletin Doc 47 7815, 12/31/17
- PCCD Body-Worn Camera (BWC) Policy Recommendations

PROVIDING YOUR INFORMATION

Please send your information to:

Christopher J. Braun M.S. IT
Technology Coordinator Pennsylvania Chiefs of Police Association
3905 N. Front Street, Harrisburg, PA 17110
Email: cjbraun@pachiefs.org

The preferred method is email or in a digital format. However, all information provided will be used. Please include the name of a contact, phone number, email address and website.
Deadline: Please send your information by 4 PM January 25, 2019.

Request For Information

Police Body Worn Cameras

APPENDIX

PA Title 18 CHAPTER 57 WIRETAPPING AND ELECTRONIC SURVEILLANCE

CHAPTER 57

WIRETAPPING AND ELECTRONIC SURVEILLANCE

Subchapter

A. General Provisions

B. Wire, Electronic or Oral Communication

C. Stored Wire and Electronic Communications and Transactional Records Access

D. Mobile Tracking Devices

E. Pen Registers, Trap and Trace Devices and Telecommunication Identification Interception Devices

F. Miscellaneous

Enactment. Present Chapter 57 was added October 4, 1978, P.L.831, No.164, effective in 60 days.

Prior Provisions. Former Chapter 57, which related to invasion of privacy, was added December 6, 1972, P.L.1482, No.334, and repealed October 4, 1978, P.L.831, No.164, effective in 60 days.

Cross References. Chapter 57 is referred to in section 1522 of Title 4 (Amusements); section 3575 of Title 42 (Judiciary and Judicial Procedure).

SUBCHAPTER A

GENERAL PROVISIONS

Sec.

5701. Short title of chapter.

5702. Definitions.

Subchapter Heading. The heading of Subchapter A was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5701. Short title of chapter.

This chapter shall be known and may be cited as the "Wiretapping and Electronic Surveillance Control Act."

§ 5702. Definitions.

As used in this chapter, the following words and phrases shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Aggrieved person." A person who was a party to any intercepted wire, electronic or oral communication or a person against whom the interception was directed.

"Aural transfer." A transfer containing the human voice at any point between and including the point of origin and the point of reception.

"Communication common carrier." Any person engaged as a common carrier for hire, in intrastate, interstate or foreign communication by wire or radio or in intrastate, interstate or foreign radio transmission of energy; however, a person engaged in radio broadcasting shall not, while so engaged, be deemed a common carrier.

"Communication service." Any service which provides to users the ability to send or receive wire or electronic communications.

"Communication system." Any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of communications and any computer facilities or related electronic equipment for the electronic storage of such communications.

"Contents." As used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication.

"Court." The Superior Court. For the purposes of Subchapter C only, the term shall mean the court of common pleas.

"Crime of violence." Any of the following:

(1) Any of the following crimes:

(i) Murder in any degree as defined in section 2502(a), (b) or (c) (relating to murder).

(ii) Voluntary manslaughter as defined in section 2503 (relating to voluntary manslaughter), drug delivery resulting in death as defined in section 2506(a) (relating to drug delivery resulting in death), aggravated assault as defined in section 2702(a)(1) or (2) (relating to aggravated assault), kidnapping as defined in section 2901(a) or (a.1) (relating to kidnapping), rape as defined in section 3121(a), (c) or (d) (relating to rape), involuntary deviate sexual intercourse as defined in section 3123(a), (b) or (c) (relating to involuntary deviate sexual intercourse), sexual assault as defined in section 3124.1 (relating to sexual assault), aggravated indecent assault as defined in section 3125(a) or (b) (relating to aggravated indecent assault), incest as defined in section 4302(a) or (b) (relating to incest), arson as defined in section 3301(a) (relating to arson and related offenses), burglary as defined in section 3502(a)(1) (relating to burglary), robbery as defined in section 3701(a)(1)(i), (ii) or (iii) (relating to robbery) or robbery of a motor vehicle as defined in section 3702(a) (relating to robbery of a motor vehicle).

(iii) Intimidation of witness or victim as defined in section 4952(a) and (b) (relating to intimidation of witnesses or victims).

(iv) Retaliation against witness, victim or party as defined in section 4953(a) and (b) (relating to retaliation against witness, victim or party).

(v) Criminal attempt as defined in section 901(a) (relating to criminal attempt), criminal solicitation as defined in section 902(a) (relating to criminal solicitation) or criminal conspiracy as defined in section 903(a) (relating to criminal conspiracy) to commit any of the offenses specified in this definition.

(2) Any offense equivalent to an offense under paragraph (1) under the laws of this Commonwealth in effect at the time of the commission of that offense or under the laws of another jurisdiction.

"Electronic communication." 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 photo-optical system, except:

(1) (Deleted by amendment).

(2) Any wire or oral communication.

(3) Any communication made through a tone-only paging device.

(4) Any communication from a tracking device (as defined in this section).

"Electronic communication service." (Deleted by amendment).

"Electronic communication system." (Deleted by amendment).

"Electronic, mechanical or other device." Any device or apparatus, including, but not limited to, an induction coil or a telecommunication identification interception device, that can be used to intercept a wire, electronic or oral communication other than:

(1) Any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service 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 being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

(2) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

(3) Equipment or devices used to conduct interceptions under section 5704(15) (relating to exceptions to prohibition of interception and disclosure of communications).

"Electronic storage."

(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.

(2) Any storage of such a communication by an electronic communication service for purpose of backup protection of the communication.

"Home." The residence of a nonconsenting party to an interception, provided that access to the residence is not generally permitted to members of the public and the party has a reasonable expectation of privacy in the residence under the circumstances.

"In-progress trace." The determination of the origin of a telephonic communication to a known telephone during an interception.

"Intercept." Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. The term shall include the point at which the contents of the communication are monitored by investigative or law enforcement officers. The term shall not include the acquisition of the contents of a communication made through any electronic, mechanical or other device or telephone instrument to an investigative or law enforcement officer, or between a person and an investigative or law enforcement officer, where the investigative or law enforcement officer poses as an actual person who is the intended recipient of the communication, provided that the Attorney General, a deputy attorney general designated in writing by the Attorney General, a district attorney or an assistant district attorney designated in writing by a district attorney of the county wherein the investigative or law enforcement officer is to receive or make the communication has reviewed the facts and is satisfied that the communication involves suspected criminal activities and has given prior approval for the communication.

"Investigative or law enforcement officer." Any officer of the United States, of another state or political subdivision thereof or of the Commonwealth or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter or an equivalent crime in another jurisdiction, and any attorney authorized by law to prosecute or participate in the prosecution of such offense.

"Judge." When referring to a judge authorized to receive applications for, and to enter, orders authorizing interceptions of wire, electronic or oral communications pursuant to Subchapter B (relating to wire, electronic or oral communication), any judge of the Superior Court.

"Mobile communications tracking information." Information generated by a communication common carrier or a communication service which indicates the location of an electronic device supported by the communication common carrier or communication service.

"One call system." A communication system established by users to provide a single telephone number for contractors or designers or any other person to call notifying users of the caller's intent to engage in demolition or excavation work.

"Oral communication." Any oral communication uttered by a person possessing an expectation that such communication is not subject to interception under circumstances justifying such expectation. The term does not include the following:

(1) An electronic communication.

(2) A communication made in the presence of a law enforcement officer on official duty who is in uniform or otherwise clearly identifiable as a law enforcement officer and who is using an electronic, mechanical or other device which has been approved under section 5706(b)(4) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the communication in the course of law enforcement duties. As used in this paragraph only, "law enforcement officer" means a member of the Pennsylvania State Police, an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training), a sheriff or a deputy sheriff.

"Organized crime."

(1) The unlawful activity of an association trafficking in illegal goods or services, including but not limited to, gambling, prostitution, loan sharking, controlled substances, labor racketeering, or other unlawful activities; or

(2) any continuing criminal conspiracy or other unlawful practice which has as its objective:

(i) large economic gain through fraudulent or coercive practices; or

(ii) improper governmental influence.

"Pen register." A device which is used to capture, record or decode electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire or electronic communications, on the targeted telephone. The term includes a device which is used to record or decode electronic or other impulses which identify the existence of incoming and outgoing wire or electronic communications on the targeted telephone. The term does not include a device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communication service provided by the 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 business.

"Person." 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.

"Readily accessible to the general public." As used with respect to a radio communication, that such communication is not:

(1) scrambled or encrypted;

(2) transmitted using modulation techniques of which the essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;

(3) carried on a subscriber or other signal subsidiary to a radio transmission;

(4) transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication; or

(5) transmitted on frequencies allocated under 47 CFR Parts 25, 74D, E, F or 94, unless, in the case of a communication transmitted on a frequency allocated under Part 74 which is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

"Remote computing service." The provision to the public of computer storage or processing services by means of an electronic communications system.

"Signed, written record." A memorialization of the contents of any wire, electronic or oral communication intercepted in accordance with this subchapter, including the name of the investigative or law enforcement officer who transcribed the record, kept in electronic, paper or any form. The signature of the transcribing officer shall not be required to be written, but may be electronic.

"State." Any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico and any territory or possession of the United States.

"Suspected criminal activity." A particular offense that has been, is or is about to occur as set forth under section 5709(3)(ii) (relating to application for order), any communications to be intercepted as set forth under section 5709(3)(iii) or any of the criminal activity set forth under section 5709(3)(iv) establishing probable cause for the issuance of an order.

"Telecommunication identification interception device." Any equipment or device capable of intercepting any electronic communication which contains any electronic serial number, mobile

identification number, personal identification number or other identification number assigned by a telecommunication service provider for activation or operation of a telecommunication device.

"Tracking device." An electronic or mechanical device which permits only the tracking of the movement of a person or object.

"Trap and trace device." 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 communication was transmitted. The term includes caller ID, deluxe caller ID or any other features available to ascertain the telephone number, location or subscriber information of a facility contacting the facility whose communications are to be intercepted.

"User." Any person or entity who:

(1) uses an electronic communication service; and

(2) is duly authorized by the provider of the service to engage in the use.

"Wire communication." Any aural transfer made in whole or in part through the use of facilities for the transmission of communication by wire, cable or other like connection between the point of origin and the point of reception, including the use of such a connection in a switching station, furnished or operated by a telephone, telegraph or radio company for hire as a communication common carrier.

(Dec. 23, 1981, P.L.593, No.175, eff. 60 days; Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days; July 7, 2017, P.L.304, No.22, eff. 60 days)

2017 Amendment. Act 22 amended the def. of "oral communication."

2012 Amendment. Act 202 amended the defs. of "intercept," "trap and trace device" and "wire communication," added the defs. of "communication service," "communication system," "crime of violence," "mobile communications tracking information" and "signed, written record" and deleted the defs. of "electronic communication service" and "electronic communication system."

2002 Amendment. Act 162 added the def. of "suspected criminal activity."

1998 Amendment. Act 19 amended the defs. of "electronic communication," "electronic, mechanical or other device," "intercept," "investigative or law enforcement officer," "judge," "pen register" and "wire communication" and added the defs. of "home," "state" and "telecommunication identification interception device."

Cross References. Section 5702 is referred to in sections 911, 5706, 5903, 6321 of this title; section 901 of Title 34 (Game); section 67A07 of Title 42 (Judiciary and Judicial Procedure); sections 57A12, 57B02 of Title 53 (Municipalities Generally); section 2604.1 of Title 66 (Public Utilities).

SUBCHAPTER B

WIRE, ELECTRONIC OR ORAL COMMUNICATION

Sec.

5728. Injunction against illegal interception.

Subchapter Heading. The heading of Subchapter B was added October 21, 1988, P.L.1000, No.115, effective immediately.

Cross References. Subchapter B is referred to in section 5702 of this title.

§ 5703. Interception, disclosure or use of wire, electronic or oral communications.

Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he:

(1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication;

(2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or

(3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

§ 5704. Exceptions to prohibition of interception and disclosure of communications.

It shall not be unlawful and no prior court approval shall be required under this chapter for:

(1) An operator of a switchboard, or an officer, agent or employee of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire 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 wire or electronic communication service. However, no provider of wire or electronic communication service shall utilize service observing or random monitoring except for mechanical or service quality control checks.

(2) Any investigative or law enforcement officer or any person acting at the direction or request of an investigative or law enforcement officer to intercept a wire, electronic or oral communication involving suspected criminal activities, including, but not limited to, the crimes enumerated in section 5708 (relating to order authorizing interception of wire, electronic or oral communications), where:

(i) (Deleted by amendment).

(ii) one of the parties to the communication has given prior consent to such interception. However, no interception under this paragraph shall be made unless the Attorney General or a deputy attorney general designated in writing by the Attorney General, or the district attorney, or an assistant district attorney designated in writing by the district attorney, of the county wherein the interception is to be initiated, has reviewed the facts and is satisfied that the consent is voluntary and has given prior approval for the interception; however, such interception shall be subject to the recording and record keeping requirements of section 5714(a) (relating to recording of intercepted communications) and that the Attorney General, deputy attorney general, district attorney or assistant district attorney authorizing the interception shall be the custodian of recorded evidence obtained therefrom;

(iii) the investigative or law enforcement officer meets in person with a suspected felon and wears a concealed electronic or mechanical device capable of intercepting or recording oral communications. However, no interception under this subparagraph may be used in any criminal prosecution except for a prosecution involving harm done to the investigative or law enforcement officer. This subparagraph shall not be construed to limit the interception and disclosure authority provided for in this subchapter; or

(iv) the requirements of this subparagraph are met. If an oral interception otherwise authorized under this paragraph will take place in the home of a nonconsenting party, then, in addition to the requirements of subparagraph (ii), the interception shall not be conducted until an order is first obtained from the president judge, or his designee who shall also be a judge, of a court of common pleas, authorizing such in-home interception, based upon an affidavit by an investigative or law enforcement officer that establishes probable cause for the issuance of such an order. No such order or affidavit shall be required where probable cause and exigent circumstances exist. For the purposes of this paragraph, an oral interception shall be deemed to take place in the home of a nonconsenting party only if both the consenting and nonconsenting parties are physically present in the home at the time of the interception.

(3) Police and emergency communications systems to record telephone communications coming into and going out of the communications system of the Pennsylvania Emergency Management Agency or a police department, fire department or county emergency center, if:

(i) the telephones thereof are limited to the exclusive use of the communication system for administrative purposes and provided the communication system employs a periodic warning which indicates to the parties to the conversation that the call is being recorded;

(ii) all recordings made pursuant to this clause, all notes made therefrom, and all transcriptions thereof may be destroyed at any time, unless required with regard to a pending matter; and

(iii) at least one nonrecorded telephone line is made available for public use at the Pennsylvania Emergency Management Agency and at each police department, fire department or county emergency center.

(4) A person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception.

(5) Any investigative or law enforcement officer, or communication common carrier acting at the direction of an investigative or law enforcement officer or in the normal course of its business, to use a pen register, trap and trace device or telecommunication identification interception device as provided in Subchapter E (relating to pen registers, trap and trace devices and telecommunication identification interception devices).

(6) Personnel of any public utility to record telephone conversations with utility customers or the general public relating to receiving and dispatching of emergency and service calls provided there is, during such recording, a periodic warning which indicates to the parties to the conversation that the call is being recorded.

(7) A user, or any officer, employee or agent of such user, to record telephone communications between himself and a contractor or designer, or any officer, employee or agent of such contractor or designer, pertaining to excavation or demolition work or other related matters, if the user or its agent indicates to the parties to the conversation that the call will be or is being recorded. As used in this paragraph, the terms "user," "contractor," "demolition work," "designer" and "excavation work" shall have the meanings given to them in the act of December 10, 1974 (P.L.852, No.287), referred to as

the Underground Utility Line Protection Law; and a one call system shall be considered for this purpose to be an agent of any user which is a member thereof.

(8) A provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the 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 the service.

(9) A person or entity providing electronic communication service to the public to divulge the contents of any such communication:

(i) as otherwise authorized in this section or section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence);

(ii) with the lawful consent of the originator or any addressee or intended recipient of the communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward the 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.

A person or entity providing electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one directed to the person or entity, or an agent thereof) while in transmission of that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.

(10) Any person:

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

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

(A) by a station for the use of the general public, or which relates to ships, aircraft, vehicles or persons in distress;

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

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

(D) by any marine or aeronautical communication system;

(iii) to engage in any conduct which:

(A) is prohibited by section 633 of the Communications Act of 1934 (48 Stat. 1105, 47 U.S.C. § 553); or

(B) is excepted from the application of section 705(a) of the Communications Act of 1934 (47 U.S.C. § 605(a)) by section 705(b) of that act (47 U.S.C. § 605(b)); or

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

(11) Other users of the same frequency to intercept any radio communication made through a system which utilizes frequencies monitored by individuals engaged in the provisions or use of the system, if the communication is not scrambled or encrypted.

(12) Any investigative or law enforcement officer or any person acting at the direction or request of an investigative or law enforcement officer to intercept a wire or oral communication involving suspected criminal activities where the officer or the person is a party to the communication and there is reasonable cause to believe that:

(i) the other party to the communication is either:

(A) holding a hostage; or

(B) has barricaded himself and taken a position of confinement to avoid apprehension; and

(ii) that party:

(A) may resist with the use of weapons; or

(B) is threatening suicide or harm to himself or others.

(13) An investigative officer, a law enforcement officer or employees of the Department of Corrections for State correctional facilities to intercept, record, monitor or divulge any oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The Department of Corrections shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging any oral communication, electronic communication or wire communication from or to an inmate in a State correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their oral communication, electronic communication or wire communication may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the Department of Corrections shall not intercept, record, monitor or divulge an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The Department of Corrections shall promulgate guidelines to implement the provisions of this paragraph for State correctional facilities.

(14) An investigative officer, a law enforcement officer or employees of a county correctional facility to intercept, record, monitor or divulge an oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The county correctional facility shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging an oral communication, electronic communication or wire communication from or to an inmate in a county correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their oral communications, electronic communications or wire communications may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the county correctional facility shall not intercept, record, monitor or divulge an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The superintendent, warden or a designee of the superintendent or warden or other chief administrative official of the county correctional system shall promulgate guidelines to implement the provisions of this paragraph for county correctional facilities.

(15) The personnel of a business engaged in telephone marketing or telephone customer service by means of wire, oral or electronic communication to intercept such marketing or customer service communications where such interception is made for the sole purpose of training, quality control or monitoring by the business, provided that one party involved in the communications has consented to such intercept. Any communications recorded pursuant to this paragraph may only be used by the business for the purpose of training or quality control. Unless otherwise required by Federal or State law, communications recorded pursuant to this paragraph shall be destroyed within one year from the date of recording.

(16) (Deleted by amendment).

(17) Any victim, witness or private detective licensed under the act of August 21, 1953 (P.L.1273, No.361), known as The Private Detective Act of 1953, to intercept the contents of any wire, electronic or oral communication, if that person is under a reasonable suspicion that the intercepted party is committing, about to commit or has committed a crime of violence and there is reason to believe that evidence of the crime of violence may be obtained from the interception.

(18) A person to intercept oral communications for disciplinary or security purposes on a school bus or school vehicle, as those terms are defined in 75 Pa.C.S. § 102 (relating to definitions), if all of the following conditions are met:

(i) The school board has adopted a policy that authorizes audio interception on school buses or school vehicles for disciplinary or security purposes.

(ii) Each school year, the school board includes the policy in a student handbook and in any other publication of the school entity that sets forth the comprehensive rules, procedures and standards of conduct for the school entity.

(iii) The school board posts a notice that students may be audiotaped, which notice is clearly visible on each school bus or school vehicle that is furnished with audio-recording equipment.

(iv) The school entity posts a notice of the policy on the school entity's publicly accessible Internet website.

This paragraph shall not apply when a school bus or school vehicle is used for a purpose that is not school related.

(July 10, 1981, P.L.227, No.72, eff. 60 days; Dec. 23, 1981, P.L.593, No.175, eff. 60 days; Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Sept. 26, 1995, 1st Sp.Sess., P.L.1056, No.20, eff. 60 days; Dec. 19, 1996, P.L.1458, No.186, eff. 60 days; Feb. 18, 1998, P.L.102, No.19, eff. imd.; June 11, 2002, P.L.367, No.52, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days; Feb. 4, 2014, P.L.21, No.9; June 23, 2016, P.L.392, No.56, eff. 60 days; July 7, 2017, P.L.304, No.22, eff. 60 days)

2017 Amendment. Act 22 amended pars. (13) and (14) and deleted par. (16).

2016 Amendment. Act 56 amended par. (18).

2014 Amendment. Act 9 amended par. (16) and added par. (18), effective in 60 days as to par. (16) and immediately as to the remainder of the section.

2012 Amendment. Act 202 amended pars. (2)(ii), (12)(ii), (13)(i)(B) and (14)(i)(B) and added par. (17).

1998 Amendment. Act 19 amended the intro. par. and pars. (2), (5) and (9) and added par. (15).

1996 Amendment. Act 186 amended par. (2) and added par. (14).

1995 Amendment. Act 20, 1st Sp.Sess., added par. (13).

Cross References. Section 5704 is referred to in sections 5702, 5706, 5717, 5720, 5721.1, 5742, 5747, 5749, 5782 of this title; section 901 of Title 30 (Fish); section 901 of Title 34 (Game).

§ 5705. Possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices and telecommunication identification interception devices.

Except as otherwise specifically provided in section 5706 (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), a person is guilty of a felony of the third degree if he does any of the following:

(1) Intentionally possesses an 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 a wire, electronic or oral communication.

(2) Intentionally sells, transfers or distributes an 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 a wire, electronic or oral communication.

(3) Intentionally manufactures or assembles an 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 a wire, electronic or oral communication.

(4) Intentionally places in any newspaper, magazine, handbill, or other publication any advertisement of an 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 a wire, electronic or oral communication or of an electronic, mechanical or other device where such advertisement promotes the use of such device for the purpose of the surreptitious interception of a wire, electronic or oral communication.

(5) Intentionally possesses a telecommunication identification interception device.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended the section heading and added par. (5).

§ 5706. Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices.

(a) Unlawful activities.--It shall not be unlawful under this chapter for:

(1) 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 the wire or electronic communication service; or

(2) a person under contract with the United States, the Commonwealth or a political subdivision thereof, a state or a political subdivision thereof, or an officer, agent or employee of the United States, the Commonwealth or a political subdivision thereof, or a state or a political subdivision thereof,

to possess, sell, distribute, manufacture, assemble or advertise an electronic, mechanical or other device, while acting in furtherance of the appropriate activities of the United States, the Commonwealth or a political subdivision thereof, a state or a political subdivision thereof or a provider of wire or electronic communication service.

(b) Responsibility.--

(1) Except as provided under paragraph (2), the Attorney General and the district attorney or their designees so designated in writing shall have the sole responsibility to buy, possess and loan any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12) (relating to exceptions to prohibition of interception and disclosure of communications), 5712 (relating to issuance of order and effect), 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations).

(2) The division or bureau or section of the Pennsylvania State Police responsible for conducting the training in the technical aspects of wiretapping and electronic surveillance as required by section 5724 (relating to training) may buy and possess any electronic, mechanical or other device which is to

be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 for the purpose of training. However, any electronic, mechanical or other device bought or possessed under this provision may be loaned to or used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 only upon written approval by the Attorney General or a deputy attorney general designated in writing by the Attorney General or the district attorney or an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur.

(3) With the permission of the Attorney General or a district attorney who has designated any supervising law enforcement officer for purposes of interceptions as authorized under section 5713.1, the law enforcement agency which employs the supervising law enforcement officer may buy, possess, loan or borrow any electronic, mechanical or other device which is to be used by investigative or law enforcement officers at the direction of the supervising law enforcement officer solely for the purpose of interception as authorized under sections 5704(12) and 5713.1.

(4) The Pennsylvania State Police shall annually establish equipment standards for any electronic, mechanical or other device which is to be used by law enforcement officers for purposes of recording a communication under circumstances within paragraph (2) of the definition of "oral communication" in section 5702 (relating to definitions). The equipment standards shall be published annually in the Pennsylvania Bulletin.

(5) The Pennsylvania State Police shall annually establish and publish standards in the Pennsylvania Bulletin for the secure onsite and off-site storage of an audio recording made in accordance with paragraph (4) or any accompanying video recording. The standards shall comply with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

(6) A vendor to law enforcement agencies which stores data related to audio recordings and video recordings shall, at a minimum, comply with the standards set forth by the Pennsylvania State Police under paragraphs (4) and (5). Law enforcement agencies under contract with a vendor for the storage of data before the effective date of this paragraph shall comply with paragraphs (4) and (5) and this paragraph upon expiration or renewal of the contract.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; June 11, 2002, P.L.367, No.52, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days; July 7, 2017, P.L.304, No.22, eff. 60 days)

2017 Amendment. Act 22 amended subsec. (b).

Cross References. Section 5706 is referred to in sections 5702, 5705 of this title; section 901 of Title 34 (Game); section 67A07 of Title 42 (Judiciary and Judicial Procedure).

§ 5707. Seizure and forfeiture of electronic, mechanical or other devices.

Any electronic, mechanical or other device possessed, used, sent, distributed, manufactured, or assembled in violation of this chapter is hereby declared to be contraband and may be seized and forfeited to the Commonwealth in accordance with 42 Pa.C.S. §§ 5803 (relating to asset forfeiture), 5805 (relating to forfeiture procedure), 5806 (relating to motion for return of property), 5807 (relating to restrictions on use), 5807.1 (relating to prohibition on adoptive seizures) and 5808 (relating to exceptions).

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; June 29, 2017, P.L.247, No.13, eff. July 1, 2017)

Cross References. Section 5707 is referred to in section 5803 of Title 42 (Judiciary and Judicial Procedure).

§ 5708. Order authorizing interception of wire, electronic or oral communications.

The Attorney General, or, during the absence or incapacity of the Attorney General, a deputy attorney general designated in writing by the Attorney General, or the district attorney or, during the absence or incapacity of the district attorney, an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur, may make written application to any Superior Court judge for an order authorizing the interception of a wire, electronic or oral communication by the investigative or law enforcement officers or agency having responsibility for an investigation involving suspected criminal activities when such interception may provide evidence of the commission of any of the following offenses, or may provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of the following offenses:

(1) Under this title:

Section 911 (relating to corrupt organizations)

Section 2501 (relating to criminal homicide)

Section 2502 (relating to murder)

Section 2503 (relating to voluntary manslaughter)

Section 2702 (relating to aggravated assault)

Section 2706 (relating to terroristic threats)

Section 2709.1 (relating to stalking)

Section 2716 (relating to weapons of mass destruction)

Section 2901 (relating to kidnapping)

Section 3011 (relating to trafficking in individuals)

Section 3012 (relating to involuntary servitude)

Section 3121 (relating to rape)

Section 3123 (relating to involuntary deviate sexual intercourse)

Section 3124.1 (relating to sexual assault)

Section 3125 (relating to aggravated indecent assault)

Section 3301 (relating to arson and related offenses)

Section 3302 (relating to causing or risking catastrophe)

Section 3502 (relating to burglary)

Section 3701 (relating to robbery)

Section 3921 (relating to theft by unlawful taking or disposition)

Section 3922 (relating to theft by deception)

Section 3923 (relating to theft by extortion)

Section 4701 (relating to bribery in official and political matters)

Section 4702 (relating to threats and other improper influence in official and political matters)

Section 5512 (relating to lotteries, etc.)

Section 5513 (relating to gambling devices, gambling, etc.)

Section 5514 (relating to pool selling and bookmaking)

Section 5516 (relating to facsimile weapons of mass destruction)

Section 6318 (relating to unlawful contact with minor)

(2) Under this title, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 910 (relating to manufacture, distribution or possession of devices for theft of telecommunications services)

Section 2709(a)(4), (5), (6) or (7) (relating to harassment)

Section 3925 (relating to receiving stolen property)

Section 3926 (relating to theft of services)

Section 3927 (relating to theft by failure to make required disposition of funds received)

Section 3933 (relating to unlawful use of computer)

Section 4108 (relating to commercial bribery and breach of duty to act disinterestedly)

Section 4109 (relating to rigging publicly exhibited contest)

Section 4117 (relating to insurance fraud)

Section 4305 (relating to dealing in infant children)

Section 4902 (relating to perjury)

Section 4909 (relating to witness or informant taking bribe)

Section 4911 (relating to tampering with public records or information)

Section 4952 (relating to intimidation of witnesses or victims)

Section 4953 (relating to retaliation against witness or victim)

Section 5101 (relating to obstructing administration of law or other governmental function)

Section 5111 (relating to dealing in proceeds of unlawful activities)

Section 5121 (relating to escape)

Section 5902 (relating to prostitution and related offenses)

Section 5903 (relating to obscene and other sexual materials and performances)

Section 7313 (relating to buying or exchanging Federal Supplemental Nutrition Assistance Program (SNAP) benefit coupons, stamps, authorization cards or access devices)

(3) Under the act of March 4, 1971 (P.L.6, No.2), known as the Tax Reform Code of 1971, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 1272 (relating to sales of unstamped cigarettes)

Section 1273 (relating to possession of unstamped cigarettes)

Section 1274 (relating to counterfeiting)

(4) Any offense set forth under section 13(a) of the act of April 14, 1972 (P.L.233, No.64), known as The Controlled Substance, Drug, Device and Cosmetic Act, not including the offense described in clause (31) of section 13(a).

(5) Any offense set forth under the act of November 15, 1972 (P.L.1227, No.272).

(6) Any conspiracy to commit any of the offenses set forth in this section.

(7) Under the act of November 24, 1998 (P.L.874, No.110), known as the Motor Vehicle Chop Shop and Illegally Obtained and Altered Property Act.

(Dec. 2, 1983, P.L.248, No.67, eff. imd.; Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 2, 1990, P.L.4, No.3, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Dec. 21, 1998, P.L.1086, No.145, eff. 60 days; June 28, 2002, P.L.481, No.82, eff. 60 days; Nov. 20, 2002, P.L.1104, No.134, eff. 60 days; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days; Dec. 9, 2002, P.L.1759, No.218, eff. 60 days; Nov. 9, 2006, P.L.1340, No.139, eff. 60 days; July 2, 2014, P.L.945, No.105, eff. 60 days; Oct. 24, 2018, P.L.1159, No.160, eff. 60 days)

2018 Amendment. Act 160 amended par. (2).

2014 Amendment. Act 105 amended par. (1).

2002 Amendments. Act 82 amended par. (1), Act 134 amended par. (1), Act 162 amended the entire section and Act 218 amended pars. (1) and (2). Act 162 overlooked the amendment by Act 134 and Act 218 overlooked the amendments by Acts 134 and 162, but the amendments do not conflict in substance and have been given effect in setting forth the text of section 5708.

Effective Date. After January 20, 2003, and before February 7, 2003, section 5708 will reflect only the amendment by Act 134, as follows:

§ 5708. Order authorizing interception of wire, electronic or oral communications.

The Attorney General, or, during the absence or incapacity of the Attorney General, a deputy attorney general designated in writing by the Attorney General, or the district attorney or, during the absence or incapacity of the district attorney, an assistant district attorney designated in writing by the district attorney of the county wherein the interception is to be made, may make written application to any Superior Court judge for an order authorizing the interception of a wire, electronic or oral communication by the investigative or law enforcement officers or agency having responsibility for an investigation involving suspected criminal activities when such interception may provide evidence of the commission of any of the following offenses, or may provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of the following offenses:

(1) Under this title:

Section 911 (relating to corrupt organizations)

Section 2501 (relating to criminal homicide)

Section 2502 (relating to murder)

Section 2503 (relating to voluntary manslaughter)

Section 2702 (relating to aggravated assault)

Section 2706 (relating to terroristic threats)

Section 2709(b) (relating to harassment and stalking)

Section 2716 (relating to weapons of mass destruction)

Section 2901 (relating to kidnapping)

Section 3121 (relating to rape)

Section 3123 (relating to involuntary deviate sexual intercourse)

Section 3124.1 (relating to sexual assault)

Section 3125 (relating to aggravated indecent assault)

Section 3301 (relating to arson and related offenses)

Section 3302 (relating to causing or risking catastrophe)

Section 3502 (relating to burglary)

Section 3701 (relating to robbery)

Section 3921 (relating to theft by unlawful taking or disposition)

Section 3922 (relating to theft by deception)

Section 3923 (relating to theft by extortion)

Section 4701 (relating to bribery in official and political matters)

Section 4702 (relating to threats and other improper influence in official and political matters)

Section 5512 (relating to lotteries, etc.)

Section 5513 (relating to gambling devices, gambling, etc.)

Section 5514 (relating to pool selling and bookmaking)

Section 5516 (relating to facsimile weapons of mass destruction)

Section 6318 (relating to unlawful contact with minor)

(2) Under this title, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 910 (relating to manufacture, distribution or possession of devices for theft of telecommunications services)

Section 3925 (relating to receiving stolen property)

Section 3926 (relating to theft of services)

Section 3927 (relating to theft by failure to make required disposition of funds received)

Section 3933 (relating to unlawful use of computer)

Section 4108 (relating to commercial bribery and breach of duty to act disinterestedly)

Section 4109 (relating to rigging publicly exhibited contest)

Section 4117 (relating to insurance fraud)

Section 4305 (relating to dealing in infant children)

Section 4902 (relating to perjury)

Section 4909 (relating to witness or informant taking bribe)

Section 4911 (relating to tampering with public records or information)

Section 4952 (relating to intimidation of witnesses or victims)

Section 4953 (relating to retaliation against witness or victim)

Section 5101 (relating to obstructing administration of law or other governmental function)

Section 5111 (relating to dealing in proceeds of unlawful activities)

Section 5121 (relating to escape)

Section 5504 (relating to harassment by communication or address)

Section 5902 (relating to prostitution and related offenses)

Section 5903 (relating to obscene and other sexual materials and performances)

Section 7313 (relating to buying or exchanging Federal food order coupons, stamps, authorization cards or access devices)

(3) Under the act of March 4, 1971 (P.L.6, No.2), known as the Tax Reform Code of 1971, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 1272 (relating to sales of unstamped cigarettes)

Section 1273 (relating to possession of unstamped cigarettes)

Section 1274 (relating to counterfeiting)

(4) Any offense set forth under section 13(a) of the act of April 14, 1972 (P.L.233, No.64), known as The Controlled Substance, Drug, Device and Cosmetic Act, not including the offense described in clause (31) of section 13(a).

(5) Any offense set forth under the act of November 15, 1972 (P.L.1227, No.272).

(6) Any conspiracy to commit any of the offenses set forth in this section.

(7) Under the act of November 24, 1998 (P.L.874, No.110), known as the Motor Vehicle Chop Shop and Illegally Obtained and Altered Property Act.

References in Text. The act of November 15, 1972 (P.L.1227, No.272), referred to in this section, amended the act of December 8, 1970 (P.L.874, No.276), known as The Pennsylvania Corrupt Organizations Act of 1970, which was repealed by the act of December 6, 1972 (P.L.1482, No.334). The subject matter is now contained in section 911 of Title 18.

Section 3933, referred to in this section, is repealed.

Section 5504, referred to in this section, is repealed.

The act of November 24, 1998 (P.L.874, No.110), known as the Vehicle Chop Shop and Illegally Obtained and Altered Property Act, referred to in paragraph (7), was repealed by the act of October 25, 2012 (P.L.1645, No.203). The subject matter is now contained in Chapter 77 of this title.

Cross References. Section 5708 is referred to in sections 5704, 5710, 5713, 5742 of this title.

§ 5709. Application for order.

Each application for an order of authorization to intercept a wire, electronic or oral communication shall be made in writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the suspected criminal activity has been, is or is about to occur and shall contain all of the following:

(1) A statement of the authority of the applicant to make such application.

(2) A statement of the identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to intercept a wire, electronic or oral communication is sought.

(3) A sworn statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application, which shall include:

(i) The identity of the particular person, if known, committing the offense and whose communications are to be intercepted.

(ii) The details as to the particular offense that has been, is being, or is about to be committed.

(iii) The particular type of communication to be intercepted.

(iv) A showing that there is probable cause to believe that such communication will be communicated on the wire communication facility involved or at the particular place where the oral communication is to be intercepted.

(v) The character and location of the particular wire communication facility involved or the particular place where the oral communication is to be intercepted.

(vi) A statement of the period of time for which the interception is required to be maintained, and, if the character 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 statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.

(vii) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or are too dangerous to employ.

(4) Where the application is for the renewal or extension of an order, a particular statement of facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(5) A complete statement of the facts concerning all previous applications, known to the applicant made to any court for authorization to intercept a wire, electronic or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each such application.

(6) A proposed order of authorization for consideration by the judge.

(7) Such additional testimony or documentary evidence in support of the application as the judge may require.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days)

Cross References. Section 5709 is referred to in sections 5702, 5712.1, 5713.1 of this title.

§ 5710. Grounds for entry of order.

(a) Application.--Upon consideration of an application, the judge may enter an ex parte order, as requested or as modified, authorizing the interception of wire, electronic or oral communications anywhere within the Commonwealth, if the judge determines on the basis of the facts submitted by the applicant that there is probable cause for belief that all the following conditions exist:

(1) the person whose communications are to be intercepted is committing, has or had committed or is about to commit an offense as provided in section 5708 (relating to order authorizing interception of wire, electronic or oral communications);

(2) particular communications concerning such offense may be obtained through such interception;

(3) normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

(4) the facility from which, or the place where, the wire, electronic or oral communications are to be intercepted, is, has been, or is about to be used, in connection with the commission of such offense, or is leased to, listed in the name of, or commonly used by, such person;

(5) the investigative or law enforcement officers or agency to be authorized to intercept the wire, electronic or oral communications are qualified by training and experience to execute the interception sought, and are certified under section 5724 (relating to training); and

(6) in the case of an application, other than a renewal or extension, for an order to intercept a communication of a person or on a facility which was the subject of a previous order authorizing interception, the application is based upon new evidence or information different from and in addition to the evidence or information offered to support the prior order, regardless of whether such evidence was derived from prior interceptions or from other sources.

(b) Corroborative evidence.--As part of the consideration of an application in which there is no corroborative evidence offered, the judge may inquire in camera as to the identity of any informants or any other additional information concerning the basis upon which the investigative or law enforcement officer or agency has applied for the order of authorization which the judge finds relevant in order to determine if there is probable cause pursuant to this section.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

Cross References. Section 5710 is referred to in sections 5712, 5721.1 of this title.

§ 5711. Privileged communications.

No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

§ 5712. Issuance of order and effect.

(a) Authorizing orders.--An order authorizing the interception of any wire, electronic or oral communication shall state the following:

(1) The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic or oral communications is given and the name and official identity of the person who made the application.

(2) The identity of, or a particular description of, the person, if known, whose communications are to be intercepted.

(3) The character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted.

(4) A particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates.

(5) 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.

(b) Time limits.--No order entered under this section shall authorize the interception of any wire, electronic or oral communication for a period of time in excess of that necessary under the circumstances. Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this chapter by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order. In the event the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. No order entered under this section shall authorize the interception of wire, electronic or oral communications for any period exceeding 30 days. The 30-day period begins on the day on which the investigative or law enforcement officers or agency first begins to conduct an interception under the order, or ten days after the order is entered, whichever is earlier. Extensions or renewals of such an order may be granted for additional periods of not more than 30 days each. No extension or renewal shall be granted unless an application for it is made in accordance with this section, and the judge makes the findings required by section 5710 (relating to grounds for entry of order).

(c) Responsibility.--The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

(d) Progress reports.--Whenever an order authorizing an interception is entered, 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. The reports shall be made at such intervals as the judge may require.

(e) Final report.--Whenever an interception is authorized pursuant to this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the

application for order, shall be filed with the court as soon as practicable after the authorized interception is terminated.

(f) Assistance.--An order authorizing the interception of a wire, electronic or oral communication shall, upon request of the applicant, direct that a provider of communication service 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 is affording the person whose communications are to be intercepted. The obligation of a provider of communication service under such an order may include, but is not limited to, installation of a pen register or of a trap and trace device, providing caller ID, deluxe caller ID or any other features available to ascertain the telephone number, location or subscriber information of a facility contacting the facility whose communications are to be intercepted, disclosure of a record or other information otherwise available under section 5743 (relating to requirements for governmental access), including conducting an in-progress trace during an interception, provided that such obligation of a provider of communications service is technologically feasible. The order shall apply regardless of whether the electronic service provider is headquartered within this Commonwealth, if the interception is otherwise conducted within this Commonwealth as provided under this chapter. The order regarding disclosure of a record or other information otherwise available under section 5743 shall apply to all electronic service providers who service facilities which contact or are contacted by the facility whose communications are to be intercepted, regardless of whether the order specifically names any provider of communication service. The order may specify the period of time an electronic service provider has to furnish to the applicant who requests disclosure of a record or other information otherwise available under section 5743. Any provider of communication service furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing the facilities or assistance. The service provider shall be immune from civil and criminal liability for any assistance rendered to the applicant pursuant to this section.

(g) Entry by law enforcement officers.--An order authorizing the interception of a wire, electronic or oral communication shall, if requested, authorize the entry of premises or facilities specified in subsection (a)(3), or premises necessary to obtain access to the premises or facilities specified in subsection (a)(3), by the law enforcement officers specified in subsection (a)(1), as often as necessary solely for the purposes of installing, maintaining or removing an electronic, mechanical or other device or devices provided that such entry is reasonably necessary to accomplish the purposes of this subchapter and provided that the judge who issues the order shall be notified of the time and method of each such entry prior to entry if practical and, in any case, within 48 hours of entry.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (a) intro. par. and (f).

1998 Amendment. Act 19 amended subsecs. (e), (f) and (g).

Cross References. Section 5712 is referred to in sections 5706, 5712.1, 5713.1, 5721.1 of this title.

§ 5712.1. Target-specific orders.

(a) Target-specific wiretaps.--The requirements of sections 5712(a)(3) (relating to issuance of order and effect) and 5709(3)(iv) and (v) (relating to application for order) shall not apply if:

(1) In the case of an application with respect to the interception of an oral communication, all of the following apply:

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

(ii) The judge finds the specification is not practical.

(2) In the case of an application with respect to a wire or electronic communication, all of the following apply:

(i) The application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception by changing facilities or devices.

(ii) The judge finds that the purpose has been adequately shown.

(b) Supplementary orders.--Following the issuance of a target-specific wiretap order, the judge shall sign supplementary orders upon request and in a timely manner, authorizing the investigative or law enforcement officers or agency to intercept additional communications devices or facilities upon a showing of reasonable suspicion that all of the following apply:

(1) The target of the original order has in fact changed communications devices or facilities or is presently using additional communications devices, communications facilities or places.

(2) The target of the original order is likely to use the specified communications device or facility for criminal purposes similar to or related to those specified in the original order.

(c) Application for supplementary orders.--An application for a supplementary order shall contain all of the following:

(1) The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic or oral communications is given and the name and official identity of the person who made the application.

(2) The identity of or a particular description of the person, if known, whose communications are to be intercepted.

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

(4) A showing of reasonable suspicion that the target of the original order has in fact changed communications devices or facilities.

(5) A showing of reasonable suspicion that the target of the original order is likely to use the additional facility or device or place for criminal purposes similar to or related to those specified in the original order.

(d) Time limits.--A supplementary order shall not act as an extension of the time limit identified in section 5712(b).

(e) Responsibility.--The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

(f) Progress reports.--If an order authorizing an interception is entered, 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. The reports shall be made at intervals as the judge may require.

(g) Final report.--If an interception is authorized under this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the application for order, shall be filed with the court as soon as practical after the authorized interception is terminated.

(h) Assistance.--

(1) An order authorizing the interception of a wire, electronic or oral communication shall, upon request of the applicant, direct that a provider of communication service furnish the applicant with all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the service provider is affording the person whose communications are to be intercepted.

(2) The obligation of a provider of communication service under an order may include installation of a pen register or trap and trace device and disclosure of a record or other information otherwise available under section 5743 (relating to requirements for governmental access), including conducting an in-progress trace during an interception, if the obligation of a provider of communications service is technologically feasible.

(3) A provider of communication service furnishing facilities or technical assistance shall be compensated by the applicant for reasonable expenses incurred in providing the facilities or assistance.

(4) A service provider shall be immune from civil and criminal liability for any assistance rendered to an applicant under this section.

(i) Entry by law enforcement officers.--An order authorizing the interception of a wire, electronic or oral communication shall, if requested, authorize the entry of premises or facilities specified under subsection (c)(3) or premises necessary to obtain access to the premises or facilities specified under subsection (c)(3) by law enforcement officers specified under subsection (c)(1) as often as necessary solely for the purposes of installing, maintaining or removing an electronic, mechanical or other device, if all of the following apply:

(1) The entry is reasonably necessary to accomplish the purposes of this subchapter.

(2) The judge who issues the order is notified of the time and method of each entry prior to entry within 48 hours of entry.

(Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 added section 5712.1.

§ 5713. Emergency situations.

(a) Application.--Whenever, upon informal application by the Attorney General or a designated deputy attorney general authorized in writing by the Attorney General or a district attorney or an assistant district attorney authorized in writing by the district attorney of a county wherein the suspected criminal activity has been, is or is about to occur, a judge determines there are grounds upon which an order could be issued pursuant to this chapter, and that an emergency situation exists

with respect to the investigation of an offense designated in section 5708 (relating to order authorizing interception of wire, electronic or oral communications), and involving conspiratorial activities characteristic of organized crime or a substantial danger to life or limb, dictating authorization for immediate interception of wire, electronic or oral communications before an application for an order could with due diligence be submitted to him and acted upon, the judge may grant oral approval for such interception without an order, conditioned upon the filing with him, within 48 hours thereafter, of an application for an order which, if granted, shall recite the oral approval and be retroactive to the time of such oral approval. Such interception shall immediately terminate when the communication sought is obtained or when the application for an order is denied, whichever is earlier. In the event no application for an order is made, the content of any wire, electronic or oral communication intercepted shall be treated as having been obtained in violation of this subchapter.

(b) Further proceedings.--In the event no application is made or an application made pursuant to this section is denied, the court shall cause an inventory to be served as provided in section 5716 (relating to service of inventory and inspection of intercepted communications) and shall require the tape or other recording of the intercepted communication to be delivered to, and sealed by, the court. Such evidence shall be retained by the court in accordance with section 5714 (relating to recording of intercepted communications) and the same shall not be used or disclosed in any legal proceeding except in a civil action brought by an aggrieved person pursuant to section 5725 (relating to civil action for unlawful interception, disclosure or use of wire, electronic or oral communication) or as otherwise authorized by court order. In addition to other remedies and penalties provided by this chapter, failure to effect delivery of any such tape or other recording shall be punishable as contempt by the court directing such delivery. Evidence of oral authorization to intercept wire, electronic or oral communications shall be a defense to any charge against the investigating or law enforcement officer for engaging in unlawful interception.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days)

2002 Amendment. Act 162 amended subsec. (a).

Cross References. Section 5713 is referred to in sections 5706, 5713.1, 5716, 5721.1, 5747 of this title.

§ 5713.1. Emergency hostage and barricade situations.

(a) Designation.--The Attorney General or a district attorney may designate supervising law enforcement officers for the purpose of authorizing the interception of wire or oral communications as provided in this section.

(b) Procedure.--A supervising law enforcement officer who reasonably determines that an emergency situation exists that requires a wire or oral communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and who determines that there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire or oral communication. An application for an order approving the interception must be made by the supervising law enforcement officer in accordance with section 5709 (relating to application for order) within 48 hours after the interception has occurred or begins to occur. Interceptions pursuant to this section shall be conducted in accordance with the procedures of this subchapter. Upon request of the supervising law enforcement officer who determines to authorize interceptions of wire communications under this section, a provider of electronic

communication service shall provide assistance and be compensated therefor as provided in section 5712(f) (relating to issuance of order and effect). In the absence of an order, such interception shall immediately terminate when the situation giving rise to the hostage or barricade situation ends 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 or oral communication intercepted shall be treated as having been obtained in violation of this subchapter, and an inventory shall be served as provided in section 5716 (relating to service of inventory and inspection of intercepted communications). Thereafter, the supervising law enforcement officer shall follow the procedures set forth in section 5713(b) (relating to emergency situations).

(c) Defense.--A good faith reliance on the provisions of this section shall be a complete defense to any civil or criminal action brought under this subchapter or any other statute against any law enforcement officer or agency conducting any interceptions pursuant to this section as well as a provider of electronic communication service who is required to provide assistance in conducting such interceptions upon request of a supervising law enforcement officer.

(d) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Emergency situation." Any situation where:

(1) a person is holding a hostage and is threatening serious physical injury and may resist with the use of weapons; or

(2) a person has barricaded himself and taken a position of confinement to avoid apprehension and:

(i) has the ability to resist with the use of weapons; or

(ii) is threatening suicide or harm to himself or others.

"Supervising law enforcement officer."

(1) For designations by a district attorney, any law enforcement officer trained pursuant to section 5724 (relating to training) to carry out interceptions under this section who has attained the rank of lieutenant or higher in a law enforcement agency within the county or who is in charge of a county law enforcement agency.

(2) For designations by the Attorney General, any member of the Pennsylvania State Police trained pursuant to section 5724 to carry out interceptions under this section and designated by the Commissioner of the Pennsylvania State Police who:

(i) has attained the rank of lieutenant or higher; or

(ii) is in charge of a Pennsylvania State Police barracks.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsec. (d).

1998 Amendment. Act 19 amended subsecs. (b) and (c).

1988 Amendment. Act 115 added section 5713.1.

Cross References. Section 5713.1 is referred to in sections 5706, 5716, 5721.1 of this title.

§ 5714. Recording of intercepted communications.

(a) Recording and monitoring.--Any wire, electronic or oral communication intercepted in accordance with this subchapter shall, if practicable, be recorded by tape or other comparable method. The recording shall be done in such a way as will protect it from editing or other alteration. Whenever an interception is being monitored, the monitor shall be an investigative or law enforcement officer certified under section 5724 (relating to training), and where practicable, keep a signed, written record which shall include the following:

(1) The date and hours of surveillance.

(2) The time and duration of each intercepted communication.

(3) The participant, if known, in each intercepted conversation.

(4) A summary of the content of each intercepted communication.

(b) Sealing of recordings.--Immediately upon the expiration of the order or extensions or renewals thereof, all monitor's records, tapes and other recordings shall be transferred to the judge issuing the order and sealed under his direction. Custody of the tapes, or other recordings shall be maintained wherever the court directs. They shall not be destroyed except upon an order of the court and in any event shall be kept for ten years. Duplicate tapes, or other recordings may be made for disclosure or use pursuant to section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence). The presence of the seal provided by this section, or a satisfactory explanation for its absence, shall be a prerequisite for the disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom, under section 5717(b).

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Cross References. Section 5714 is referred to in sections 5704, 5713, 5749, 5773 of this title.

§ 5715. Sealing of applications, orders and supporting papers.

Applications made, final reports, and orders granted pursuant to this subchapter and supporting papers and monitor's records shall be sealed by the court and shall be held in custody as the court shall direct and shall not be destroyed except on order of the court and in any event shall be kept for ten years. They may be disclosed only upon a showing of good cause before a court of competent jurisdiction except that any investigative or law enforcement officer may disclose such applications, orders and supporting papers and monitor's records to investigative or law enforcement officers of this or another state, any of its political subdivisions, or of the United States to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. In addition to any remedies and penalties provided by this subchapter, any violation of the provisions of this section may be punished as contempt of the court.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5716. Service of inventory and inspection of intercepted communications.

(a) Service of inventory.--Within a reasonable time but not later than 90 days after the termination of the period of the order or of extensions or renewals thereof, or the date of the denial of an order applied for under section 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations), the issuing or denying judge shall cause to be served on the

persons named in the order, application, or final report an inventory which shall include the following:

(1) Notice of the entry of the order or the application for an order denied under section 5713 or 5713.1.

(2) The date of the entry of the order or the denial of an order applied for under section 5713 or 5713.1.

(3) The period of authorized or disapproved interception.

(4) The fact that during the period wire or oral communications were or were not intercepted.

(b) Postponement.--On an ex parte showing of good cause to the issuing or denying judge the service of the inventory required by this section may be postponed for a period of 30 days. Additional postponements may be granted for periods of not more than 30 days on an ex parte showing of good cause to the issuing or denying judge.

(c) Inspections.--The court, upon the filing of a motion, shall make available to such persons or their attorneys for inspection, the intercepted communications and monitor's records to which the movant was a participant and the applications and orders.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

Cross References. Section 5716 is referred to in sections 5713, 5713.1 of this title.

§ 5717. Investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence.

(a) Law enforcement personnel.--Any investigative or law enforcement officer who, under subsection (a.1), (b), (b.1) or (c), has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, may disclose such contents or evidence 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.

(a.1) Use of information.--Any investigative or law enforcement officer who, by any means authorized by this subchapter, has obtained knowledge of the contents of any wire, electronic or oral communication or evidence derived therefrom may use such contents or evidence to the extent such use is appropriate to the proper performance of his official duties.

(b) Evidence.--Any person who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, may disclose such contents or evidence to an investigative or law enforcement officer and may disclose such contents or evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of this Commonwealth or of another state or of the United States or before any state or Federal grand jury or investigating grand jury.

(b.1) Criminal cases.--Any person who by means authorized by section 5704(17) (relating to exceptions to prohibition of interception and disclosure of communications) has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, may in addition to disclosures made under subsection (b) disclose such contents or evidence, on the condition that such disclosure is made for the purpose of providing exculpatory evidence in an open or closed criminal case.

(c) Otherwise authorized personnel.--

(1) Except as provided under paragraph (2), any person who, by any means authorized by the laws of another state or the Federal Government, has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived from any wire, electronic or oral communication, may disclose the contents or evidence to an investigative or law enforcement officer and may disclose the contents or evidence where otherwise admissible while giving testimony under oath or affirmation in any proceeding in any court of this Commonwealth.

(2) The contents of a nonconsensual interception authorized by the laws of the Federal Government or another state shall not be admissible unless the interception was authorized by a court upon a finding of probable cause that the target of the surveillance is engaged or will engage in a violation of the criminal laws of the Federal Government or any state.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsec. (a) and added subsecs. (b.1) and (c).

Cross References. Section 5717 is referred to in sections 5704, 5714, 5718, 5721.1, 5749 of this title.

§ 5718. Interception of communications relating to other offenses.

When an investigative or law enforcement officer, while engaged in court authorized interceptions of wire, electronic or oral communications in the manner authorized herein, intercepts wire, electronic or oral communications relating to offenses other than those specified in the order of authorization, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in section 5717(a) (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence). Such contents and evidence may be disclosed in testimony under oath or affirmation in any criminal proceeding in any court of this Commonwealth or of another state or of the United States or before any state or Federal grand jury when authorized by a judge who finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this subchapter. Such application shall be made as soon as practicable.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5719. Unlawful use or disclosure of existence of order concerning intercepted communication.

Except as specifically authorized pursuant to this subchapter any person who willfully uses or discloses the existence of an order authorizing interception of a wire, electronic or oral communication is guilty of a misdemeanor of the second degree.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5720. Service of copy of order and application before disclosure of intercepted communication in trial, hearing or proceeding.

The contents of any wire, electronic or oral communication intercepted in accordance with the provisions of this subchapter, or evidence derived therefrom, shall not be disclosed in any trial, hearing, or other adversary proceeding before any court of the Commonwealth unless, not less than ten days before the trial, hearing or proceeding the parties to the action have been served with a copy of the order, the accompanying application and the final report under which the interception

was authorized or, in the case of an interception under section 5704 (relating to exceptions to prohibition of interception and disclosure of communications), notice of the fact and nature of the interception. The service of inventory, order, application, and final report required by this section may be waived by the court only where it finds that the service is not feasible and that the parties will not be prejudiced by the failure to make the service.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Suspension by Court Rule. Section 5720 was suspended by Pennsylvania Rule of Juvenile Court Procedure No. 800(14), amended February 12, 2010, insofar as it is inconsistent with Rule 340(B)(6) relating to pre-adjudicatory discovery and inspection.

Section 5720 was suspended by Pennsylvania Rule of Criminal Procedure No. 1101(5), adopted March 1, 2000, insofar as it is inconsistent with Rule No. 573 only insofar as section 5720 may delay disclosure to a defendant seeking discovery under Rule No. 573(B)(1)(g).

§ 5721. Suppression of contents of intercepted communication or derivative evidence (Repealed).

1998 Repeal. Section 5721 was repealed February 18, 1998 (P.L.102, No.19), effective immediately.

§ 5721.1. Evidentiary disclosure of contents of intercepted communication or derivative evidence.

(a) Disclosure in evidence generally.--

(1) Except as provided in paragraph (2), no person shall disclose the contents of any wire, electronic or oral communication, or evidence derived therefrom, in any proceeding in any court, board or agency of this Commonwealth.

(2) Any person who has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, which is properly subject to disclosure under section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence) may also disclose such contents or evidence in any matter relating to any criminal, quasi-criminal, forfeiture, administrative enforcement or professional disciplinary proceedings in any court, board or agency of this Commonwealth or of another state or of the United States or before any state or Federal grand jury or investigating grand jury. Once such disclosure has been made, then any person may disclose the contents or evidence in any such proceeding.

(3) Notwithstanding the provisions of paragraph (2), no disclosure in any such proceeding shall be made so long as any order excluding such contents or evidence pursuant to the provisions of subsection (b) is in effect.

(b) Motion to exclude.--Any aggrieved person who is a party to any proceeding in any court, board or agency of this Commonwealth may move to exclude the contents of any wire, electronic or oral communication, or evidence derived therefrom, on any of the following grounds:

(1) Unless intercepted pursuant to an exception set forth in section 5704 (relating to exceptions to prohibition of interception and disclosure of communications), the interception was made without prior procurement of an order of authorization under section 5712 (relating to issuance of order and effect) or an order of approval under section 5713(a) (relating to emergency situations) or 5713.1(b) (relating to emergency hostage and barricade situations).

(2) The order of authorization issued under section 5712 or the order of approval issued under section 5713(a) or 5713.1(b) was not supported by probable cause with respect to the matters set forth in section 5710(a)(1) and (2) (relating to grounds for entry of order).

(3) The order of authorization issued under section 5712 is materially insufficient on its face.

(4) The interception materially deviated from the requirements of the order of authorization.

(5) With respect to interceptions pursuant to section 5704(2), the consent to the interception was coerced by the Commonwealth.

(6) Where required pursuant to section 5704(2)(iv), the interception was made without prior procurement of a court order or without probable cause.

(c) Procedure.--

(1) The motion shall be made in accordance with the applicable rules of procedure governing such proceedings. The court, board or agency, upon the filing of such motion, shall make available to the movant or his counsel the intercepted communication and evidence derived therefrom.

(2) In considering a motion to exclude under subsection (b)(2), both the written application under section 5710(a) and all matters that were presented to the judge under section 5710(b) shall be admissible.

(3) The movant shall bear the burden of proving by a preponderance of the evidence the grounds for exclusion asserted under subsection (b)(3) and (4).

(4) With respect to exclusion claims under subsection (b)(1), (2) and (5), the respondent shall bear the burden of proof by a preponderance of the evidence.

(5) With respect to exclusion claims under subsection (b)(6), the movant shall have the initial burden of demonstrating by a preponderance of the evidence that the interception took place in his home. Once he meets this burden, the burden shall shift to the respondent to demonstrate by a preponderance of the evidence that the interception was in accordance with section 5704(2)(iv).

(6) Evidence shall not be deemed to have been derived from communications excludable under subsection (b) if the respondent can demonstrate by a preponderance of the evidence that the Commonwealth or the respondent had a basis independent of the excluded communication for discovering such evidence or that such evidence would have been inevitably discovered by the Commonwealth or the respondent absent the excluded communication.

(d) Appeal.--In addition to any other right of appeal, the Commonwealth shall have the right to appeal from an order granting a motion to exclude if the official to whom the order authorizing the intercept was granted shall certify to the court that the appeal is not taken for purposes of delay. The appeal shall be taken in accordance with the provisions of Title 42 (relating to judiciary and judicial procedure).

(e) Exclusiveness of remedies and sanctions.--The remedies and sanctions described in this subchapter with respect to the interception of wire, electronic or oral communications are the only judicial remedies and sanctions for nonconstitutional violations of this subchapter involving such communications.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

1998 Amendment. Act 19 added section 5721.1.

Cross References. Section 5721.1 is referred to in section 5749 of this title.

§ 5722. Report by issuing or denying judge.

Within 30 days after the expiration of an order or an extension or renewal thereof entered under this subchapter or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the Administrative Office of Pennsylvania Courts stating the following:

(1) That an order, extension or renewal was applied for.

(2) The kind of order applied for.

(3) That the order was granted as applied for, was modified, or was denied.

(4) The period of the interceptions authorized by the order, and the number and duration of any extensions or renewals of the order.

(5) The offense specified in the order, or extension or renewal of an order.

(6) The name and official identity of the person making the application and of the investigative or law enforcement officer and agency for whom it was made.

(7) The character of the facilities from which or the place where the communications were to be intercepted.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5723. Annual reports and records of Attorney General and district attorneys.

(a) Judges.--In addition to reports required to be made by applicants pursuant to Title 18 U.S.C. § 2519, all judges who have issued orders pursuant to this title shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts. The reports by the judges shall contain the following information:

(1) The number of applications made.

(2) The number of orders issued.

(3) The effective periods of such orders.

(4) The number and duration of any renewals thereof.

(5) The crimes in connection with which the orders were sought.

(6) The names and official identity of the applicants.

(7) Such other and further particulars as the Administrative Office of Pennsylvania Courts may require.

(b) Attorney General.--In addition to reports required to be made by applicants pursuant to Title 18 U.S.C. § 2519, the Attorney General shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts and to the Judiciary Committees of the Senate and House of Representatives. The reports by the Attorney General shall contain the same information which must be reported pursuant to 18 U.S.C. § 2519(2).

(c) District attorneys.--Each district attorney shall annually provide to the Attorney General all of the foregoing information with respect to all applications authorized by that district attorney on forms prescribed by the Attorney General.

(d) Other reports.--The Chief Justice of the Supreme Court and the Attorney General shall annually report to the Governor and the General Assembly on such aspects of the operation of this chapter as they deem appropriate and make any recommendations they feel desirable as to legislative changes or improvements to effectuate the purposes of this chapter and to assure and protect individual rights.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

§ 5724. Training.

The Attorney General and the Commissioner of the Pennsylvania State Police shall establish a course of training in the legal and technical aspects of wiretapping and electronic surveillance as allowed or permitted by this subchapter, shall establish such regulations as they find necessary and proper for such training program and shall establish minimum standards for certification and periodic recertification of Commonwealth investigative or law enforcement officers as eligible to conduct wiretapping or electronic surveillance under this chapter. The Pennsylvania State Police shall charge each investigative or law enforcement officer who enrolls in this training program a reasonable enrollment fee to offset the costs of such training.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Cross References. Section 5724 is referred to in sections 5706, 5710, 5713.1, 5714, 5749 of this title.

§ 5725. Civil action for unlawful interception, disclosure or use of wire, electronic or oral communication.

(a) Cause of action.--Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person:

(1) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher.

(2) Punitive damages.

(3) A reasonable attorney's fee and other litigation costs reasonably incurred.

(b) Waiver of sovereign immunity.--To the extent that the Commonwealth and any of its officers, officials or employees would be shielded from liability under this section by the doctrine of sovereign immunity, such immunity is hereby waived for the purposes of this section.

(c) Defense.--It is a defense to an action brought pursuant to subsection (a) that the actor acted in good faith reliance on a court order or the provisions of this chapter.

(July 10, 1981, P.L.228, No.73, eff. 60 days; Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

Cross References. Section 5725 is referred to in section 5713 of this title.

§ 5726. Action for removal from office or employment.

(a) Cause of action.--Any aggrieved person shall have the right to bring an action in Commonwealth Court against any investigative or law enforcement officer, public official or public employee seeking the officer's, official's or employee's removal from office or employment on the grounds that the officer, official or employee has intentionally violated the provisions of this chapter. If the court shall conclude that such officer, official or employee has in fact intentionally violated the provisions of this chapter, the court shall order the dismissal or removal from office of said officer, official or employee.

(b) Defense.--It is a defense to an action brought pursuant to subsection (a) that the actor acted in good faith reliance on a court order or the provisions of this chapter.

(July 10, 1981, P.L.228, No.73, eff. 60 days)

§ 5727. Expiration (Repealed).

1988 Repeal. Section 5727 was repealed October 21, 1988 (P.L.1000, No.115), effective immediately.

§ 5728. 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 subchapter, the Attorney General may initiate a civil action in the Commonwealth Court to enjoin the violation. The court shall proceed as soon as practicable to the hearing and determination of the action and may, at any time before final determination, enter a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the Commonwealth or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Pennsylvania Rules of Civil Procedure, except that, if a criminal complaint has been filed against the respondent, discovery is governed by the Pennsylvania Rules of Criminal Procedure.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

1988 Amendment. Act 115 added section 5728.

SUBCHAPTER C

STORED WIRE AND ELECTRONIC COMMUNICATIONS

AND TRANSACTIONAL RECORDS ACCESS

Sec.

Enactment. Subchapter C was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5741. Unlawful access to stored communications.

(a) Offense.--Except as provided in subsection (c), it is an offense to obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage by intentionally:

(1) accessing without authorization a facility through which an electronic communication service is provided; or

(2) exceeding the scope of one's authorization to access the facility.

(b) Penalty.--

(1) If the offense is committed for the purpose of commercial advantage, malicious destruction or damage, or private commercial gain, the offender shall be subject to:

(i) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense; or

(ii) a fine of not more than $250,000 or imprisonment for not more than two years, or both, for any subsequent offense.

(2) In any other case, the offender shall be subject to a fine of not more than $5,000 or imprisonment for not more than six months, or both.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized:

(1) by the person or entity providing a wire or electronic communication service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 5743 (relating to requirements for governmental access) or 5744 (relating to backup preservation).

§ 5742. Disclosure of contents and records.

(a) Prohibitions.--Except as provided in subsection (b) and (c):

(1) A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service:

(i) On behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service.

(ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

(2) A person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service:

(i) On behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service.

(ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

(3) A person or entity providing an electronic communication service or remote computing service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to, or customer of, the service.

(b) Exceptions.--A person or entity may divulge the contents of a communication:

(1) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;

(2) as otherwise authorized in section 5704(1) (relating to prohibition of interception and disclosure of communications), 5708 (relating to order authorizing interception of wire, electronic or oral communications) or 5743 (relating to governmental access);

(3) with the lawful consent of the originator or an addressee or intended recipient of the communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward the communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of the service; or

(6) to a law enforcement agency, if the contents:

(i) Were inadvertently obtained by the service provider.

(ii) Appear to pertain to the commission of a crime.

(c) Exceptions for disclosure of records or other information.--A person or entity may divulge a record or other information pertaining to a subscriber to, or customer of, the service if any of the following paragraphs apply:

(1) A record or other information may be divulged incident to any service or other business operation or to the protection of the rights or property of the provider.

(2) A record or other information may be divulged to any of the following:

(i) An investigative or law enforcement official as authorized in section 5743.

(ii) The subscriber or customer upon request.

(iii) A third party, upon receipt from the requester of adequate proof of lawful consent from the subscriber to, or customer of, the service to release the information to the third party.

(iv) A party to a legal proceeding, upon receipt from the party of a court order entered under subsection (c.1). This subparagraph does not apply to an investigative or law enforcement official authorized under section 5743.

(3) Notwithstanding paragraph (2), a record or other information may be divulged as authorized by a Commonwealth statute or as authorized by a Commonwealth regulatory agency with oversight over the person or entity.

(4) Subject to paragraph (2), a record or other information may be divulged as authorized by Federal law or as authorized by a Federal regulatory agency having oversight over the person or entity.

(c.1) Order for release of records.--

(1) An order to divulge a record or other information pertaining to a subscriber or customer under subsection (c)(2)(iv) must be approved by a court presiding over the proceeding in which a party seeks the record or other information.

(2) The order may be issued only after the subscriber or customer received notice from the party seeking the record or other information and was given an opportunity to be heard.

(3) The court may issue a preliminary order directing the provider to furnish the court with the identity of or contact information for the subscriber or customer if the party does not possess this information.

(4) An order for disclosure of a record or other information shall be issued only if the party seeking disclosure demonstrates specific and articulable facts to show that there are reasonable grounds to believe that the record or other information sought is relevant and material to the proceeding. In making its determination, the court shall consider the totality of the circumstances, including input of the subscriber or customer, if any, and the likely impact of the provider.

(Oct. 9, 2008, P.L.1403, No.111, eff. imd.)

2008 Amendment. Act 111 amended the section heading and subsec. (a) intro. par. and added subsecs. (a)(3), (c) and (c.1).

Cross References. Section 5742 is referred to in section 5746 of this title.

§ 5743. Requirements for governmental access.

(a) Contents of communications in electronic storage.--Investigative or law enforcement officers may require the disclosure by a provider of communication service of the contents of a communication which is in electronic storage in a communication system for:

(1) One hundred eighty days or less only pursuant to a warrant issued under the Pennsylvania Rules of Criminal Procedure.

(2) More than 180 days by the means available under subsection (b).

(b) Contents of communications in a remote computing service.--

(1) Investigative or law enforcement officers may require a provider of remote computing service to disclose the contents of any communication to which this paragraph is made applicable by paragraph (2):

(i) without required notice to the subscriber or customer if the investigative or law enforcement officer obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure; or

(ii) with prior notice from the investigative or law enforcement officer to the subscriber or customer if the investigative or law enforcement officer:

(A) uses an administrative subpoena authorized by a statute or a grand jury subpoena; or

(B) obtains a court order for the disclosure under subsection (d);

except that delayed notice may be given pursuant to section 5745 (relating to delayed notice).

(2) Paragraph (1) is applicable with respect to a communication which is held or maintained on that service:

(i) On behalf of and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the remote computing service.

(ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--

(1) (Deleted by amendment).

(2) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communications covered by subsection (a) or (b), to an investigative or law enforcement officer only when the investigative or law enforcement officer:

(i) uses an administrative subpoena authorized by a statute or a grand jury subpoena;

(ii) obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure;

(iii) obtains a court order for the disclosure under subsection (d); or

(iv) has the consent of the subscriber or customer to the disclosure.

(3) An investigative or law enforcement officer receiving records or information under paragraph (2) is not required to provide notice to the customer or subscriber.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) shall be issued only if the investigative or law enforcement officer shows that there are specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order if the information or records requested are unusually voluminous in nature or compliance with the order would otherwise cause an undue burden on the provider.

(e) No cause of action against a provider disclosing information under this subchapter.--No cause of action shall lie against any provider of 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, warrant, subpoena or certification under this subchapter.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (a) and (b).

2008 Amendment. Act 111 deleted subsec. (c)(1).

1998 Amendment. Act 19 amended subsecs. (d) and (e).

Cross References. Section 5743 is referred to in sections 5712, 5712.1, 5741, 5742, 5743.1, 5744, 5745, 5746, 5747 of this title.

§ 5743.1. Administrative subpoena.

(a) Authorization.--

(1) In an ongoing investigation that monitors or utilizes online services or other means of electronic communication to identify individuals engaged in an offense involving the sexual exploitation or abuse of children, the following shall apply:

(i) The following may issue in writing and cause to be served a subpoena requiring the production and testimony under subparagraph (ii):

(A) The Attorney General.

(B) A deputy attorney general designated in writing by the Attorney General.

(C) A district attorney.

(D) An assistant district attorney designated in writing by a district attorney.

(ii) A subpoena issued under subparagraph (i) may be issued to a provider of electronic communication service or remote computing service:

(A) requiring disclosure under section 5743(c)(2) (relating to requirements for governmental access) of a subscriber or customer's name, address, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, which may be relevant to an authorized law enforcement inquiry; or

(B) requiring a custodian of the records of the provider to give testimony or affidavit concerning the production and authentication of the records or information.

(2) A subpoena under this section shall describe the information required to be produced and prescribe a return date within a reasonable period of time within which the information can be assembled and made available.

(3) If summoned to appear under paragraph (1)(ii)(B), a custodian of records subpoenaed under this section shall be paid the same fees and mileage that are paid to witnesses in the courts of this Commonwealth.

(4) Prior to the return date specified in the subpoena, the person or entity subpoenaed may, in the court of common pleas of the county in which the person or entity conducts business or resides, petition for an order modifying or setting aside the subpoena or for a prohibition of disclosure ordered by a court under paragraph (7).

(5) The following shall apply:

(i) Except as provided under subparagraph (ii), if no case or proceeding arises from the production of materials under this section within a reasonable time after the materials are produced, the agency to which the materials were delivered shall, upon written demand made by the person producing the materials, return the materials to the person.

(ii) This paragraph shall not apply if the production required was of copies rather than originals.

(6) A subpoena issued under paragraph (1) may require production as soon as possible.

(7) Without court approval, no person or entity may disclose to any other person or entity, other than to an attorney in order to obtain legal advice, the existence of the subpoena for a period of up to 90 days.

(8) A subpoena issued under this section may not require the production of anything that would be protected from production under the standards applicable to a subpoena for the production of documents issued by a court.

(b) Service.--The following shall apply:

(1) A subpoena issued under this section may be served by any person who is at least 18 years of age and is designated in the subpoena to serve it.

(2) Service upon a natural person may be made by personal delivery of the subpoena to the person.

(3) Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name by delivering the subpoena to any of the following:

(i) An officer of the entity.

(ii) A managing or general agent of the entity.

(iii) An agent authorized by appointment or by law to receive service of process in this Commonwealth.

(4) The affidavit of the person serving the subpoena entered on a true copy of the subpoena by the person serving it shall be proof of service.

(c) Enforcement.--The following shall apply:

(1) The Attorney General or a district attorney, or a designee may invoke the aid of a court of common pleas within the following jurisdictions to compel compliance with the subpoena:

(i) The jurisdiction in which the investigation is being conducted.

(ii) The jurisdiction in which the subpoenaed person resides, conducts business or may be found.

(2) The court may issue an order requiring the subpoenaed person to appear before the Attorney General or a district attorney, or a designee to produce records or to give testimony concerning the production and authentication of the records. A failure to obey the order of the court may be

punished by the court as contempt of court. All process may be served in a judicial district of the Commonwealth in which the person may be found.

(d) Immunity from civil liability.--Notwithstanding any State or local law, any person receiving a subpoena under this section who complies in good faith with the subpoena and produces the records sought shall not be liable in a court of this Commonwealth to a subscriber, customer or other person for the production or for the nondisclosure of that production to the subscriber, customer or person.

(e) Annual reports and records of Attorney General and district attorneys.--The following shall apply:

(1) On or before April 1 following the effective date of this section and annually thereafter, including the year following the expiration of this section, the Attorney General shall make a report on the operation of this section to the Judiciary Committee of the Senate and the Judiciary Committee of the House of Representatives. The reports by the Attorney General shall contain the following information for the previous calendar year:

(i) The number of administrative subpoenas issued.

(ii) The number of investigations for which an administrative subpoena was issued.

(iii) The number of court orders issued under subsections (a)(4) and (7) and (c)(2).

(iv) The number of arrests made and the type of charge filed in cases in which an administrative subpoena was issued.

(v) The number of cases in which an administrative subpoena was issued and in which no arrests or prosecutions resulted.

(2) On or before March 1 following the effective date of this section and annually thereafter, including the year following the expiration of this section, each district attorney shall provide to the Attorney General all of the information under paragraph (1) with respect to all administrative subpoenas issued by that district attorney on forms prescribed by the Attorney General.

(f) Expiration.--(Deleted by amendment).

(g) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Offense involving the sexual exploitation or abuse of children." An offense, including an attempt, conspiracy or solicitation involving any of the following, in which a victim is an individual who is under the age of 18 years:

(1) Chapter 29 (relating to kidnapping).

(2) Chapter 30 (relating to human trafficking).

(3) Chapter 31 (relating to sexual offenses).

(4) Section 6312 (relating to sexual abuse of children).

(5) Section 6318 (relating to unlawful contact with minor).

(6) Section 6320 (relating to sexual exploitation of children).

(Oct. 22, 2014, P.L.2522, No.151, eff. 60 days; Dec. 22, 2017, P.L.1218, No.67, eff. imd.)

2017 Amendment. Act 67 deleted subsec. (f).

2014 Amendment. Act 151 added section 5743.1.

§ 5744. Backup preservation.

(a) Backup preservation.--

(1) An investigative or law enforcement officer acting under section 5743(b)(2) (relating to requirements for governmental access) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of the subpoena or court order, the service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, and shall confirm to the investigative or law enforcement officer that the backup copy has been made. The backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the investigative or law enforcement officer within three days after receipt of confirmation that the backup copy has been made, unless the notice is delayed pursuant to section 5745(a) (relating to delayed notice).

(3) The service provider shall not destroy or permit the destruction of the backup copy until the later of:

(i) the delivery of the information; or

(ii) the resolution of all proceedings, including appeals of any proceeding, concerning the government's subpoena or court order.

(4) The service provider shall release the backup copy to the requesting investigative or law enforcement officer no sooner than 14 days after the officer's notice to the subscriber or customer if the service provider has not:

(i) received notice from the subscriber or customer that the subscriber or customer has challenged the officer's request; and

(ii) initiated proceedings to challenge the request of the officer.

(5) An investigative or law enforcement officer may seek to require the creation of a backup copy under paragraph (1) if in his sole discretion the officer determines that there is reason to believe that notification under section 5743 of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber, customer or service provider.

(b) Customer challenges.--

(1) Within 14 days after notice by the investigative or law enforcement officer to the subscriber or customer under subsection (a)(2), the subscriber or customer may file a motion to quash the subpoena or vacate the court order, copies to be served upon the officer and written notice of the challenge to be given to the service provider. A motion to vacate a court order shall be filed in the court which issued the order. A motion to quash a subpoena shall be filed in the court which has authority to enforce the subpoena. The motion or application shall contain an affidavit or sworn statement:

(i) stating that the applicant is a customer of or subscriber to the service from which the contents of electronic communications maintained for the applicant have been sought; and

(ii) containing the applicant's reasons for believing that the records sought are not relevant to a legitimate investigative or law enforcement inquiry or that there has not been substantial compliance with the provisions of this subchapter in some other respect.

(2) Service shall be made under this section upon the investigative or law enforcement officer by delivering or mailing by registered or certified mail a copy of the papers to the person, office or department specified in the notice which the customer has received pursuant to this subchapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Pennsylvania Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2), the court shall order the investigative or law enforcement officer to file a sworn response, which may be filed in camera if the investigative or law enforcement officer includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and responses, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the officer's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the investigative or law enforcement officer are maintained, or that there is reason to believe that the investigative or law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order the process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not reason to believe that the communications sought are relevant to a legitimate investigative or law enforcement inquiry, or that there has not been substantial compliance with the provisions of this subchapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order, and no interlocutory appeal may be taken therefrom. The Commonwealth or investigative or law enforcement officer shall have the right to appeal from an order granting a motion or application under this section.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

1998 Amendment. Act 19 amended subsec. (b).

Cross References. Section 5744 is referred to in sections 5741, 5746 of this title.

§ 5745. Delayed notice.

(a) Delay of notification.--

(1) An investigative or law enforcement officer acting under section 5743(b) (relating to requirements for governmental access) may:

(i) where a court order is sought, include in the application a request for an order delaying the notification required under section 5743(b) for a period not to exceed 90 days, which request the court shall grant if it determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2); or

(ii) where an administrative subpoena authorized by a statute or a grand jury subpoena is obtained, delay the notification required under section 5743(b) for a period not to exceed 90 days upon the

execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2).

(2) An adverse result for the purposes of paragraph (1) is:

(i) endangering the life or physical safety of an individual;

(ii) flight from prosecution;

(iii) destruction of or tampering with evidence;

(iv) intimidation of potential witnesses; or

(v) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The investigative or law enforcement officer shall maintain a true copy of a certification under paragraph (1)(ii).

(4) Extensions of the delay of notification provided for in section 5743 of up to 90 days each may be granted by the court upon application or by certification by a supervisory official in the case of an administrative or grand jury subpoena.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4), the investigative or law enforcement officer shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice which:

(i) states with reasonable specificity the nature of the investigative or law enforcement inquiry; and

(ii) informs the customer or subscriber:

(A) that information maintained for the customer or subscriber by the service provider named in the process or request was supplied to or requested by the investigative or law enforcement officer and the date on which the supplying or request took place;

(B) that notification of the customer or subscriber was delayed;

(C) the identity of the investigative or law enforcement officer or the court which made the certification or determination pursuant to which that delay was made; and

(D) which provision of this subchapter authorizes the delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent or assistant investigative agent in charge, or an equivalent, of an investigative or law enforcement agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney, or an equivalent, of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--An investigative or law enforcement officer acting under section 5743, when he is not required to notify the subscriber or customer under section 5743(b)(1), or to the extent that it may delay such notice pursuant to subsection (a), may apply to a court for an order commanding a provider of electronic communication service or remote computing service to whom a warrant, subpoena or court order is directed, not to notify any other person of the existence of the warrant, subpoena or court order for such period as the court deems appropriate. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena or court order will result in:

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of a potential witness; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Cross References. Section 5745 is referred to in sections 5743, 5744 of this title.

§ 5746. Cost reimbursement.

(a) Payment.--Except as otherwise provided in subsection (c), an investigative or law enforcement officer obtaining the contents of communications, records or other information under section 5742 (relating to disclosure of contents and records), 5743 (relating to requirements for governmental access) or 5744 (relating to backup preservation) shall reimburse the person or entity assembling or providing the information for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing and otherwise providing the information. Reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which the information may be stored.

(b) Amount.--The amount of the reimbursement provided for in subsection (a) shall be as mutually agreed upon by the investigative or law enforcement officer and the person or entity providing the information or, in the absence of agreement, shall be as determined by the court which issued the order for production of the information or the court before which a criminal prosecution relating to the information would be brought, if no court order was issued for production of the information.

(c) Applicability.--The requirement of subsection (a) does not apply with respect to records or other information maintained by a communication common carrier which relates to telephone toll records and telephone listings obtained under section 5743. The court may, however, order reimbursement as described in subsection (a) if the court determines the information required is unusually voluminous or otherwise caused an undue burden on the provider.

(d) Regulations.--The Attorney General shall promulgate regulations to implement this section.

(Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 added subsec. (d).

2008 Amendment. Act 111 amended subsec. (a).

§ 5747. Civil action.

(a) Cause of action.--Except as provided in subsection 5743(e) (relating to requirements for governmental access), any provider of electronic communication service, subscriber or customer aggrieved by any violation of this subchapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in the violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief shall include:

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) reasonable attorney fees and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

(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 5713 (relating to emergency situations); or

(3) a good faith determination that section 5704(10) (relating to exceptions to prohibitions of interception and disclosure of communications) permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this subchapter 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 discovered or had a reasonable opportunity to discover the violation.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 22, 2014, P.L.2522, No.151, eff. 60 days)

2014 Amendment. Act 151 amended subsec. (b).

1998 Amendment. Act 19 amended subsec. (d).

§ 5748. Exclusivity of remedies.

The remedies and sanctions described in this subchapter are the only judicial remedies and sanctions for nonconstitutional violations of this subchapter.

§ 5749. Retention of certain records.

(a) Retention.--The commander shall maintain all recordings of oral communications intercepted under section 5704(16) (relating to exceptions to prohibition of interception and disclosure of communications) for a minimum of 31 days after the date of the interception. All recordings made under section 5704(16) shall be recorded over or otherwise destroyed no later than 90 days after the date of the recording unless any of the following apply:

(1) The contents of the recording result in the issuance of a citation. Except as otherwise authorized under this subsection, any recording maintained under this paragraph shall be recorded over or destroyed no later than 90 days after the conclusion of the proceedings related to the citation. All recordings under this paragraph shall be maintained in accordance with section 5714(a) (relating to recording of intercepted communications), except that monitors need not be certified under section 5724 (relating to training).

(2) The commander or a law enforcement officer on the recording believes that the contents of the recording or evidence derived from the recording may be necessary in a proceeding for which disclosure is authorized under section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence) or 5721.1 (relating to evidentiary disclosure of contents of intercepted communication or derivative evidence) or in a civil proceeding.

All recordings under this paragraph shall be maintained in accordance with section 5714(a), except that monitors need not be certified under section 5724.

(3) A criminal defendant who is a participant on the recording reasonably believes that the recording may be useful for its evidentiary value at some later time in a specific criminal proceeding and, no later than 30 days following the filing of criminal charges, provides written notice to the commander indicating a desire that the recording be maintained. The written notice must specify the date, time and location of the recording; the names of the parties involved; and, if known, the case docket number.

(4) An individual who is a participant on the recording intends to pursue a civil action or has already initiated a civil action and, no later than 30 days after the date of the recording, gives written notice to the commander indicating a desire that the recording be maintained. The written notice must specify the date, time and location of the recording; the names of the parties involved; and, if a civil action has been initiated, the case caption and docket number.

(5) The commander intends to use the recording for training purposes.

(b) Disclosure.--In addition to any disclosure authorized under sections 5717 and 5721.1, any recording maintained:

(1) Under subsection (a)(4) shall be disclosed pursuant to an order of court or as required by the Pennsylvania Rules of Civil Procedure or the Pennsylvania Rules of Evidence; and

(2) Under subsection (a)(5) shall be disclosed consistent with written consent obtained from the law enforcement officer and all participants.

(c) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Commander." The:

(1) commissioner or a designee, if the recording at issue was made by a member of the Pennsylvania State Police; or

(2) chief or a designee of the law enforcement agency which made the recording at issue.

"Law enforcement officer." A member of the Pennsylvania State Police or an individual employed as a police officer who is required to be trained under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training).

(June 11, 2002, P.L.370, No.53, eff. imd.)

2002 Amendment. Act 53 added section 5749. Section 3 of Act 53 provided that section 5749 shall apply upon the enactment of a statute providing for the intercepting and recording of oral communications under 18 Pa.C.S. § 5704. Act 52 of 2002, effective June 11, 2002, added provisions relating to the intercepting and recording of oral communications under 18 Pa.C.S. § 5704.

References in Text. The reference to "commissioner" in par. (1) of the def. of "commander" in subsec. (c) probably should have been a reference to Commissioner of the Pennsylvania State Police.

Cross References. Section 5749 is referred to in section 5782 of this title.

SUBCHAPTER D

MOBILE TRACKING DEVICES

Sec.

5761. Mobile tracking devices.

Enactment. Subchapter D was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5761. Mobile tracking devices.

(a) Authority to issue.--Orders for the installation and use of mobile tracking devices may be issued by a court of common pleas.

(b) Jurisdiction.--Orders permitted by this section may authorize the use of mobile tracking devices if the device is installed and monitored within this Commonwealth. The court issuing the order must have jurisdiction over the offense under investigation.

(c) Standard for issuance of order.--An order authorizing the use of one or more mobile tracking devices may be issued to an investigative or law enforcement officer by the court of common pleas upon written application. Each application shall be by written affidavit, signed and sworn to or affirmed before the court of common pleas. The affidavit shall:

(1) state the name and department, agency or address of the affiant;

(2) identify the vehicles, containers or items to which, in which or on which the mobile tracking device shall be attached or be placed, and the names of the owners or possessors of the vehicles, containers or items;

(3) state the jurisdictional area in which the vehicles, containers or items are expected to be found; and

(4) provide a statement setting forth all facts and circumstances which provide the applicant with probable cause that criminal activity has been, is or will be in progress and that the use of a mobile tracking device will yield information relevant to the investigation of the criminal activity.

(d) Notice.--The court of common pleas shall be notified in writing within 72 hours of the time the mobile tracking device has been activated in place on or within the vehicles, containers or items.

(e) Term of authorization.--Authorization by the court of common pleas for the use of the mobile tracking device may continue for a period of 90 days from the placement of the device. An extension for an additional 90 days may be granted upon good cause shown.

(f) Removal of device.--Wherever practicable, the mobile tracking device shall be removed after the authorization period expires. If removal is not practicable, monitoring of the mobile tracking device shall cease at the expiration of the authorization order.

(g) Movement of device.--Movement of the tracking device within an area protected by a reasonable expectation of privacy shall not be monitored absent exigent circumstances or an order supported by probable cause that criminal activity has been, is or will be in progress in the protected area and that

the use of a mobile tracking device in the protected area will yield information relevant to the investigation of the criminal activity.

(Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (b) and (c)(4).

SUBCHAPTER E

PEN REGISTERS, TRAP AND TRACE DEVICES

AND TELECOMMUNICATION IDENTIFICATION

INTERCEPTION DEVICES

Sec.

Enactment. Subchapter E was added October 21, 1988, P.L.1000, No.115, effective immediately.

Subchapter Heading. The heading of Subchapter E was amended February 18, 1998, P.L.102, No.19, effective immediately.

Cross References. Subchapter E is referred to in section 5704 of this title.

§ 5771. General prohibition on use of certain devices and exception.

(a) General rule.--Except as provided in this section, no person may install or use a pen register or a trap and trace device or a telecommunication identification interception device without first obtaining a court order under section 5773 (relating to issuance of an order for use of certain devices).

(b) Exception.--The prohibition of subsection (a) does not apply with respect to the use of a pen register, a trap and trace device or a telecommunication identification interception 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 the provider, or to the protection of users of the service from abuse of service or unlawful use of service;

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

(3) with the consent of the user of the service.

(b.1) Limitation.--A government agency authorized to install and use a pen register under this chapter 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.

(c) Penalty.--Whoever intentionally and knowingly violates subsection (a) is guilty of a misdemeanor of the third degree.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Cross References. Section 5771 is referred to in section 5773 of this title.

§ 5772. Application for an order for use of certain devices.

(a) Application.--The Attorney General or a deputy attorney general designated in writing by the Attorney General or a district attorney or an assistant district attorney designated in writing by the district attorney may make application for an order or an extension of an order under section 5773 (relating to issuance of an order for use of certain devices) authorizing or approving disclosure of mobile communications tracking information or, if necessary, the production and disclosure of mobile communications tracking information, the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device under this subchapter, in writing, under oath or equivalent affirmation, to a court of common pleas having jurisdiction over the offense under investigation or to any Superior Court judge when an application for an order authorizing interception of communications is or has been made for the targeted telephone or another application for interception under this subchapter has been made involving the same investigation.

(b) Contents of application.--An application under subsection (a) shall include:

(1) The identity and authority of the attorney making the application and the identity of the investigative or law enforcement agency conducting the investigation.

(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.

(3) An affidavit by an investigative or law enforcement officer which establishes probable cause for the issuance of an order or extension of an order under section 5773.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsec. (a).

1998 Amendment. Act 19 amended the section heading and subsec. (a).

Cross References. Section 5772 is referred to in section 5773 of this title.

§ 5773. Issuance of an order for use of certain devices.

(a) In general.--Upon an application made under section 5772 (relating to application for an order for use of certain devices), the court shall enter an ex parte order authorizing the disclosure of mobile

communications tracking information, the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device within this Commonwealth if the court finds that there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained by such installation and use on the targeted telephone. If exigent circumstances exist, the court may verbally authorize the disclosure of mobile communications tracking information, the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device. The written order authorizing the disclosure must be entered within 72 hours of the court's verbal authorization.

(b) Contents of order.--An order issued under this section shall:

(1) Specify:

(i) That there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained from the targeted telephone.

(ii) The identity, if known, of the person to whom is leased or in whose name is listed the targeted telephone, or, in the case of the use of a telecommunication identification interception device, the identity, if known, of the person or persons using the targeted telephone.

(iii) The identity, if known, of the person who is the subject of the criminal investigation.

(iv) In the use of pen registers and trap and trace devices only, the physical location of the targeted telephone.

(v) A statement of the offense to which the information likely to be obtained by the pen register, trap and trace device or the telecommunication identification interception device relates.

(2) Direct, upon the request of the applicant, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the pen register under section 5771 (relating to general prohibition on use of certain devices and exception).

(3) In the case of a telecommunication identification interception device, direct that all interceptions be recorded and monitored in accordance with section 5714(a)(1) and (2) and (b) (relating to recording of intercepted communications).

(c) Time period and extensions.--

(1) An order issued under this section shall authorize the installation and use of a pen register, trap and trace device or a telecommunication identification interception device for a period not to exceed 60 days.

(2) Extensions of such an order may be granted but only upon an application for an order under section 5772 and upon the judicial finding required by subsection (a). The period of each extension shall be for a period not to exceed 30 days.

(d) Nondisclosure of existence of pen register, trap and trace device or a telecommunication identification interception device.--An order authorizing or approving the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device shall direct that:

(1) The order be sealed until otherwise ordered by the court.

(2) The person owning or leasing the targeted telephone, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register, trap and trace

device or telecommunication identification interception device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (a) and (c).

Cross References. Section 5773 is referred to in sections 5771, 5772, 5774 of this title.

§ 5774. Assistance in installation and use of certain devices.

(a) Pen register.--Upon the request of an applicant under this subchapter, a provider of wire or electronic communication service, landlord, custodian or other person shall forthwith provide 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 assistance is directed by a court order as provided in section 5773(b)(2) (relating to issuance of an order for use of certain devices).

(b) Trap and trace device.--Upon the request of an applicant under this subchapter, a provider of a wire or electronic communication service, landlord, custodian or other person shall install the device forthwith on the appropriate line and shall furnish 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 installation and assistance are directed by a court order as provided in section 5773. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the applicant designated in the court order at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation.--A provider of 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 reasonable expenses incurred in providing the facilities and assistance.

(d) No cause of action against a provider disclosing information under this subchapter.--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 subchapter.

(e) Defense.--A good faith reliance on a court order or a statutory authorization is a complete defense against any civil or criminal action brought under this subchapter or any other law.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5775. Reports concerning certain devices.

(a) Attorney General.--The Attorney General shall annually report to the Administrative Office of Pennsylvania Courts on the number of orders for pen registers, trap and trace devices and telecommunication identification interception devices applied for by investigative or law enforcement agencies of the Commonwealth or its political subdivisions.

(b) District attorney.--Each district attorney shall annually provide to the Attorney General information on the number of orders for pen registers, trap and trace devices and telecommunication identification interception devices applied for on forms prescribed by the Attorney General.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

SUBCHAPTER F

MISCELLANEOUS

Sec.

Enactment. Subchapter F was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5781. Expiration of chapter.

This chapter expires December 31, 2023, unless extended by statute.

(Dec. 12, 1994, P.L.1248, No.148, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Nov. 29, 2004, P.L.1349, No.173, eff. imd.; Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Nov. 27, 2013, P.L.1147, No.102, eff. imd.; July 7, 2017, P.L.304, No.22, eff. 60 days)

§ 5782. Regulations.

The commissioner of the Pennsylvania State Police, in consultation with the Attorney General, shall promulgate regulations consistent with sections 5704(16) (relating to exceptions to prohibition of interception and disclosure of communications) and 5749 (relating to retention of certain records) setting forth procedures to be followed by law enforcement officers regarding the interception, maintenance and destruction of recordings made under section 5704(16).

(June 11, 2002, P.L.370, No.53, eff. imd.)

2002 Amendment. Act 53 added section 5782. Section 3 of Act 53 provided that section 5782 shall apply upon the enactment of a statute providing for the intercepting and recording of oral communications under 18 Pa.C.S. § 5704. Act 52 of 2002, effective June 11, 2002, added provisions relating to the intercepting and recording of oral communications under 18 Pa.C.S. § 5704.

PA ACT 22, 2017

CRIMES CODE (18 PA.C.S.) AND JUDICIAL CODE (42 PA.C.S.) - OMBINUS AMENDMENTS

Act of Jul. 7, 2017, P.L. 304, No. 22

Cl. 18

Session of 2017

No. 2017-22

SB 560

AN ACT

Amending Titles 18 (Crimes and Offenses) and 42 (Judiciary and Judicial Procedure) of the Pennsylvania Consolidated Statutes, in wiretapping and electronic surveillance, further providing for definitions, for exceptions to prohibition of interception and disclosure of communications, for exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices and for expiration of chapter; and providing for recordings by law enforcement officers.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. The definition of "oral communication" in section 5702 of Title 18 of the Pennsylvania Consolidated Statutes is amended to read:

§ 5702. Definitions.

As used in this chapter, the following words and phrases shall have the meanings given to them in this section unless the context clearly indicates otherwise:

* * *

"Oral communication." Any oral communication uttered by a person possessing an expectation that such communication is not subject to interception under circumstances justifying such expectation. The term does not include [any electronic communication.] the following:

(1) An electronic communication.

(2) A communication made in the presence of a law enforcement officer on official duty who is in uniform or otherwise clearly identifiable as a law enforcement officer and who is using an electronic, mechanical or other device which has been approved under section 5706(b)(4) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the communication in the course of law enforcement duties. As used in this paragraph only, "law enforcement officer" means a member of the Pennsylvania State Police, an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training), a sheriff or a deputy sheriff.

* * *

Section 2. Sections 5704(13), (14) and (16), 5706(b) and 5781 of Title 18 are amended to read:

§ 5704. Exceptions to prohibition of interception and disclosure of communications.

It shall not be unlawful and no prior court approval shall be required under this chapter for:

* * *

(13) An investigative officer, a law enforcement officer or employees of the Department of Corrections for State correctional facilities to intercept, record, monitor or divulge any [telephone calls] oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The Department of Corrections shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging any [telephone calls] oral communication, electronic communication or wire communication from or to an inmate in a State correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their [telephone conversations] oral communication, electronic communication or wire communication may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording [a telephone conversation] an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded [telephone conversation] oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the Department of Corrections shall not intercept, record, monitor or divulge [any conversation] an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) [Persons who are calling in to a facility to speak to an inmate shall be notified that the call may be recorded or monitored.] Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The Department of Corrections shall promulgate guidelines to implement the provisions of this paragraph for State correctional facilities.

(14) An investigative officer, a law enforcement officer or employees of a county correctional facility to intercept, record, monitor or divulge [any telephone calls] an oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The county correctional facility shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging [any telephone calls] an oral communication, electronic communication or wire communication from or to an inmate in a county correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their [telephone conversations] oral communications, electronic communications or wire communications may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording [a telephone conversation] an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded [telephone conversation] oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the county correctional facility shall not intercept, record, monitor or divulge [any conversation] an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) [Persons who are calling into a facility to speak to an inmate shall be notified that the call may be recorded or monitored.] Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The superintendent, warden or a designee of the superintendent or warden or other chief administrative official of the county correctional system shall promulgate guidelines to implement the provisions of this paragraph for county correctional facilities.

* * *

[(16) A law enforcement officer, whether or not certified under section 5724 (relating to training), acting in the performance of his official duties to intercept and record an oral communication between individuals in accordance with the following:

(i) At the time of the interception, the oral communication does not occur inside the residence of any of the individuals.

(ii) At the time of the interception, the law enforcement officer:

(A) is in uniform or otherwise clearly identifiable as a law enforcement officer;

(B) is in close proximity to the individuals' oral communication;

(C) is using an electronic, mechanical or other device which has been approved under section 5706(b)(4) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the oral communication; and

(D) informs, as soon as reasonably practicable, the individuals identifiably present that he has intercepted and recorded the oral communication.

(iii) As used in this paragraph, the term "law enforcement officer" means a member of the Pennsylvania State Police or an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training).]

* * *

§ 5706. Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices.

* * *

(b) Responsibility.--

(1) Except as provided under paragraph (2), the Attorney General and the district attorney or their designees so designated in writing shall have the sole responsibility to buy, possess and loan any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12) (relating to exceptions to prohibition of interception and disclosure of communications), 5712 (relating to issuance of order and effect), 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations).

(2) The division or bureau or section of the Pennsylvania State Police responsible for conducting the training in the technical aspects of wiretapping and electronic surveillance as required by section 5724 (relating to training) may buy and possess any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 for the purpose of training. However, any electronic, mechanical or other device bought or possessed under this provision may be loaned to or used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 only upon written approval by the Attorney General or a deputy attorney general designated in writing by the Attorney General or the district attorney or an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur.

(3) With the permission of the Attorney General or a district attorney who has designated any supervising law enforcement officer for purposes of interceptions as authorized under section 5713.1, the law enforcement agency which employs the supervising law enforcement officer may buy, possess, loan or borrow any electronic, mechanical or other device which is to be used by investigative or law enforcement officers at the direction of the supervising law enforcement officer solely for the purpose of interception as authorized under sections 5704(12) and 5713.1.

(4) The Pennsylvania State Police shall annually establish equipment standards for any electronic, mechanical or other device which is to be used by law enforcement officers for purposes of [interception as authorized under section 5704(16).] recording a communication under circumstances within paragraph (2) of the definition of "oral communication" in section 5702 (relating to definitions). The equipment standards shall be published annually in the Pennsylvania Bulletin.

(5) The Pennsylvania State Police shall annually establish and publish standards in the Pennsylvania Bulletin for the secure onsite and off-site storage of an audio recording made in accordance with paragraph (4) or any accompanying video recording. The standards shall comply with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

(6) A vendor to law enforcement agencies which stores data related to audio recordings and video recordings shall, at a minimum, comply with the standards set forth by the Pennsylvania State Police under paragraphs (4) and (5). Law enforcement agencies under contract with a vendor for the storage of data before the effective date of this paragraph shall comply with paragraphs (4) and (5) and this paragraph upon expiration or renewal of the contract.

§ 5781. Expiration of chapter.

This chapter expires December 31, [2018] 2023, unless extended by statute.

Section 3. Title 42 is amended by adding a chapter to read:

CHAPTER 67A

RECORDINGS BY LAW ENFORCEMENT OFFICERS

Sec.

67A01. Definitions.

67A02. Scope of chapter.

67A03. Requests for law enforcement audio recordings or video recordings.

67A04. Law enforcement review.

67A05. Procedure.

67A06. Petition for judicial review.

67A07. Audio recording or video recording policies.

67A08. Construction.

67A09. Applicability.

§ 67A01. Definitions.

The following words and phrases when used in this chapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Confidential information." Any of the following:

(1) The identity of a confidential source.

(2) The identity of a suspect or witness to whom confidentiality has been assured.

(3) Information made confidential by law or court order.

"Information pertaining to an investigation." An audio recording or video recording which contains any of the following:

(1) Complaints or depictions of criminal conduct, including all actions or statements made before or after the criminal conduct that are part of or relate to the same incident or occurrence.

(2) Upon disclosure, information that would:

(i) reveal the institution, progress or result of a criminal investigation;

(ii) deprive an individual of the right to a fair trial or an impartial adjudication;

(iii) impair the ability of the Attorney General, a district attorney or a law enforcement officer to locate a defendant or codefendant;

(iv) hinder the ability of the Attorney General, a district attorney or a law enforcement officer to secure an arrest, prosecution or conviction; or

(v) endanger the life or physical safety of an individual.

(3) Upon disclosure, information that would:

(i) Reveal the institution, progress or result of an agency investigation.

(ii) Deprive a person of the right to an impartial administrative adjudication.

(iii) Constitute an unwarranted invasion of privacy.

(iv) Hinder an agency's ability to secure an administrative or civil sanction.

(v) Endanger the life or physical safety of an individual.

"Law enforcement agency." The Office of Attorney General, a district attorney's office or an agency that employs a law enforcement officer.

"Law enforcement officer." An officer of the United States, the Commonwealth or a political subdivision thereof, another state or political subdivision thereof or who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter or an equivalent

crime in another jurisdiction, a sheriff or deputy sheriff and any attorney authorized by law to prosecute or participate in the prosecution of the offense.

"Victim." An individual who was subjected to an act that was committed by another individual, including a juvenile, which constitutes any of the following:

(1) An offense committed under any of the following:

(i) The act of April 14, 1972 (P.L.233, No.64), known as The Controlled Substance, Drug, Device and Cosmetic Act.

(ii) 18 Pa.C.S. (relating to crimes and offenses).

(iii) 30 Pa.C.S. § 5502 (relating to operating watercraft under influence of alcohol or controlled substance).

(iv) 30 Pa.C.S. § 5502.1 (relating to homicide by watercraft while operating under influence).

(v) 75 Pa.C.S. § 3732 (relating to homicide by vehicle).

(vi) 75 Pa.C.S. § 3735 (relating to homicide by vehicle while driving under influence).

(vii) 75 Pa.C.S. § 3735.1 (relating to aggravated assault by vehicle while driving under the influence).

(viii) 75 Pa.C.S. § 3742 (relating to accidents involving death or personal injury).

(ix) 75 Pa.C.S. Ch. 38 (relating to driving after imbibing alcohol or utilizing drugs).

(x) Any other Federal or State law.

(2) An offense similar to an offense listed under paragraph (1) committed outside of this Commonwealth.

(3) An offense which would constitute grounds for the issuance of relief under Chapter 62A (relating to protection of victims of sexual violence or intimidation) or 23 Pa.C.S. Ch. 61 (relating to protection from abuse).

(4) An offense against a resident of this Commonwealth which is an act of international terrorism.

"Victim information." Information that would disclose the identity or jeopardize the safety of a victim.

§ 67A02. Scope of chapter.

(a) Exemption.--The provisions of this chapter, and not the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law, shall apply to any audio recording or video recording made by a law enforcement agency.

(b) Limitation.--Nothing in this chapter nor the Right-to-Know Law shall establish a right to production of an audio recording or video recording made inside a facility owned or operated by a law enforcement agency or to any communications between or within law enforcement agencies concerning an audio or video recording.

§ 67A03. Requests for law enforcement audio recordings or video recordings.

The following shall apply:

(1) An individual who requests an audio recording or video recording made by a law enforcement agency shall, within 60 days of the date when the audio recording or video recording was made, serve

a written request to the individual who is designated as the open-records officer for the law enforcement agency under section 502 of the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law. Service is effective upon receipt of the written request by the open-records officer from personal delivery or certified mail with proof of service.

(2) The request under paragraph (1) shall specify with particularity the incident or event that is the subject of the audio recording or video recording, including the date, time and location of the incident or event.

(3) The request shall include a statement describing the requester's relationship to the incident or event that is the subject of the audio or video recording.

(4) If the incident or event that is the subject of the audio recording or video recording occurred inside a residence, the request shall identify each individual who was present at the time of the audio recording or video recording unless not known and not reasonably ascertainable.

§ 67A04. Law enforcement review.

(a) Determination.--Except as provided in this section, if a law enforcement agency determines that an audio recording or video recording contains potential evidence in a criminal matter, information pertaining to an investigation or a matter in which a criminal charge has been filed, confidential information or victim information and the reasonable redaction of the audio or video recording would not safeguard potential evidence, information pertaining to an investigation, confidential information or victim information, the law enforcement agency shall deny the request in writing. The written denial shall state that reasonable redaction of the audio recording or video recording will not safeguard potential evidence, information pertaining to an investigation, confidential information or victim information.

(b) Agreement.--A law enforcement agency may enter into a memorandum of understanding with the Attorney General or the district attorney with jurisdiction to:

(1) ensure consultation regarding the reviewing of audio recordings or video recordings in order to make a determination; or

(2) require the Attorney General or district attorney with jurisdiction to issue a denial permitted under subsection (a).

§ 67A05. Procedure.

(a) Disclosure.--A law enforcement agency that receives a request under section 67A03 (relating to requests for law enforcement audio recordings or video recordings) for an audio recording or video recording shall provide the audio recording or video recording or identify in writing the basis for denying the request within 30 days of receiving the request, unless the requester and law enforcement agency agree to a longer time period. If an agreement under section 67A04(b)(2) (relating to law enforcement review) is in effect between the law enforcement agency and the Attorney General or district attorney with jurisdiction, then an agreement to a longer time period must be between the requester and the Attorney General or district attorney with jurisdiction.

(b) Denials by operation of law.--The request under section 67A03 shall be deemed denied by operation of law if the law enforcement agency does not provide the audio recording or video recording to the requester or explain why the request is denied within the time period specified or agreed to under subsection (a).

(c) Preservation.--A law enforcement agency that has received a request for an audio recording or video recording shall preserve the unaltered audio recording or video recording that has been requested for no less than the time periods provided in this chapter for service of and responses to written requests for the production of the audio recording or video recording and any period within which a petition for judicial review is allowable or pending.

(d) Fees.--A law enforcement agency may establish reasonable fees relating to the costs incurred to disclose audio recordings or video recordings. The fees shall be paid by the requesting party at the time of disclosure of the audio recording or video recording.

(e) Construction.--Nothing in this section shall be construed to prohibit a law enforcement agency from redacting an audio recording or video recording in order to protect potential evidence in a criminal matter, information pertaining to an investigation, confidential information or victim information.

§ 67A06. Petition for judicial review.

(a) Petition.--

(1) If a request under section 67A03 (relating to requests for law enforcement audio recordings or video recordings) is denied, the requester may file a petition for judicial review in the court of common pleas with jurisdiction within 30 days of the date of denial.

(2) The respondent to a petition filed under this section shall be the entity that denied the request for the audio recording or video recording under section 67A05(a) (relating to procedure) unless the request is denied under section 67A05(b), in which case the law enforcement agency that created the audio recording or video recording shall be the respondent.

(b) Duties of petitioner.--A petitioner under this section shall have the following duties:

(1) The petitioner shall pay a filing fee of $125.

(2) If the incident or event that is the subject of the request occurred inside a residence, the petitioner shall certify that notice of the petition has been served or that service was attempted on each individual who was present at the time of the audio recording or video recording and on the owner and occupant of the residence. Notice shall not be required under this paragraph if the identity of an individual present or the location is unknown and not reasonably ascertainable by the petitioner. Service shall be effective upon receipt from personal delivery or certified mail with proof of service.

(3) The petitioner shall include with the petition a copy of the written request under section 67A03 that was served on the law enforcement agency and any written responses to the request that were received.

(4) The petitioner shall serve the petition on the open- records officer of the respondent within five days of the date that the petitioner files the petition with the court of common pleas with jurisdiction, and service shall be effective upon receipt by the open-records officer for personal delivery or certified mail with proof of service.

(c) Intervention as matter of right.--If not a respondent, a prosecuting attorney with jurisdiction may intervene in the action as a matter of right.

(d) Summary dismissal.--It shall be grounds for summary dismissal of a petition filed under this section if:

(1) the request to the law enforcement agency under section 67A03 or the filing of the petition under subsection (a) is untimely;

(2) the request to the law enforcement agency failed to describe with sufficient particularity the incident or event that is the subject of the audio recording or video recording, including the date, time and location of the incident or event; or

(3) the petitioner has not complied with the requirements of subsection (b)(1), (2), (3) and (4).

(e) Approval.--A court of common pleas with jurisdiction may grant a petition under this section, in whole or in part, and order the disclosure of the audio recording or video recording only if the court determines that the petitioner has established all of the following by a preponderance of the evidence:

(1) The request was not denied under section 67A04 (relating to law enforcement review) or the request was denied under section 67A04 and the court of common pleas with jurisdiction determines that the denial was arbitrary and capricious.

(2) The public interest in disclosure of the audio recording or video recording or the interest of the petitioner outweighs the interests of the Commonwealth, the law enforcement agency or an individual's interest in nondisclosure. In making a determination under this paragraph, the court of common pleas may consider the public's interest in understanding how law enforcement officers interact with the public, the interests of crime victims, law enforcement and others with respect to safety and privacy and the resources available to review and disclose the audio recording or video recording.

§ 67A07. Audio recording or video recording policies.

(a) Policies.--A municipal law enforcement agency or sheriff that makes audio recordings or video recordings of communications under circumstances within paragraph (2) of the definition of "oral communication" in 18 Pa.C.S. § 5702 (relating to definitions) shall comply with the guidelines established under 18 Pa.C.S. § 5706(b)(4), (5) and (6) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) and shall establish written policies, which shall be public, for the following:

(1) The training of law enforcement officers authorized to make audio recordings or video recordings.

(2) The time periods when an electronic, mechanical or other device shall be in operation to make audio recordings or video recordings.

(3) The proper use, maintenance and storage of the electronic, mechanical or other device to make audio recordings or video recordings, including equipment inspections and audits and procedures to address malfunctioning equipment.

(4) The information collected from audio recordings or video recordings, including the information's storage, accessibility and retrieval.

(5) Electronic records retention.

(6) The use of facial recognition software or programs.

(7) A statement that a violation of the agency's policy subjects the violator to the agency's disciplinary policy.

(8) Supervisory responsibilities.

(b) Pennsylvania Commission on Crime and Delinquency.--The Pennsylvania Commission on Crime and Delinquency is authorized to condition funding or a grant related to the implementation, use, maintenance or storage of body-worn cameras or recordings from body-worn cameras on the following:

(1) Requiring the grantee to have protocols, guidelines or written policies related to the implementation, use, maintenance or storage of body-worn cameras.

(2) Requiring that such protocols, guidelines or written policies are publicly accessible, including being retrievable on a municipal website.

(3) Ensuring that the protocols, guidelines or written policies substantially comply with applicable recommendations by the commission.

§ 67A08. Construction.

The following shall apply:

(1) Nothing in this chapter shall be construed to alter the responsibilities of parties to any criminal or civil litigation to exchange information in accordance with applicable rules of procedure.

(2) Nothing in this chapter shall be construed to preclude a prosecuting attorney with jurisdiction or a law enforcement agency from disclosing an audio recording or video recording in the absence of a written request or beyond the time periods stated in this chapter.

(3) The prosecuting attorney with jurisdiction must agree in writing to the disclosure by a law enforcement agency if the prosecuting attorney determines that:

(i) the audio recording or video recording contains potential evidence in a criminal matter, information pertaining to an investigation, confidential information or victim information; and

(ii) reasonable redaction of the audio recording or video recording will not safeguard the potential evidence, information pertaining to an investigation, confidential information or victim information.

§ 67A09. Applicability.

Nothing in this chapter shall apply to an audio recording or video recording that is otherwise prohibited or protected from disclosure under any other Federal or State law.

Section 4. This act shall take effect in 60 days.

APPROVED--The 7th day of July, A.D. 2017.TOM WOLF

Pennsylvania Bulletins

NOTICES

STATE POLICE

Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems

[45 Pa.B. 5482]

The State Police, under the authority of 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4) (relating to exceptions to prohibition of interception and disclosure of communications; and exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), has approved, until the next comprehensive list is published, subject to interim amendment, the following equipment standards for electronic, mechanical or other devices (mobile video recording systems) which may be used by law enforcement officers for the purpose of interception as authorized under 18 Pa.C.S. § 5704(16). Mobile video recording systems must consist of the following components.

Vehicle-Mounted Mobile Video Recording Systems Overview

Vehicle-Mounted Mobile Video Recording Systems shall be defined as those which are permanently mounted in vehicles requiring the operator to possess a Class A, B, C or M Pennsylvania Driver's License, as defined in 75 Pa.C.S. § 1504 (relating to classes of licenses). The design of the vehicle-mounted mobile video recording system must use technology, which includes a camera, monitor, wireless voice transmitter/receiver and a recording device with a secure protective enclosure for the recording device, electronics and receiver components. The vehicle-mounted mobile video recording system must be powered from a standard automotive vehicle operating at 11 to 16.5 volts DC, negative ground. Current drain on the vehicle electrical system must not exceed 3.0 amps. The system must operate over the following temperature range: -4°F to 130°F (-20°C to 55°C).

Camera

The camera component must have the following features:

A. Auto focus and auto iris.

B. Flexible mounting bracket to allow manual aiming controls.

C. Auto zoom (automatic zoom in then back out to normal distance).

D. Minimum sensitivity rating of 2.0 lux.

E. Minimum horizontal resolution of 330 TV lines.

Monitor

The monitor component must have the following features:

A. Controls for picture brightness and contrast.

B. Capability of being switched off without affecting recording.

C. A speaker and volume control system.

The monitor must be capable of displaying:

A. Camera image (live).

B. Previously recorded information from the recording unit.

C. Date and time.

D. Recording index indicator.

E. In-car/wireless microphone activity indicator.

Wireless Voice Transmitter/Receiver

The wireless voice transmitter/receiver must have the following features:

A. Battery powered wireless microphone transmitter.

B. Antenna incorporated into the microphone.

C. A plug-in connector and a clothing clip on the microphone.

D. FCC: Type acceptable under 47 CFR Part 74, Subpart H (relating to low power auxiliary stations).

E. The transmitter must not have recording capabilities.

F. The wireless audio system must be equipped with either a digital coded squelch or a PL tone squelch circuit to prevent accidental activation of the record mode in stray RF fields.

Recording Device

The recording device must be capable of recording onto tape or other comparable media and have the following features:

A. Enclosed in a secure housing protected from physical damage and unauthorized access.

B. Capable of recording audio and video for a minimum of 2 continuous hours.

C. Record time/date, recording index and remote microphone indicator.

D. Record over protection.

System Control

The control console must be mounted within easy reach of the operator. The control console must contain the controls to operate the following functions:

A. Power.

B. Record.

C. Play.

D. Rewind.

E. Fast forward.

F. Pause.

The State Police, under the authority of 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4), has approved for use, until the next comprehensive list is published, subject to interim amendment, the following list of approved vehicle-mounted mobile video recording systems which meet the minimum equipment standards in this notice.

System 7, Mobile Vision, Boonton, NJ
Eyewitness, Kustom Signals, Lenexa, KS
Patrol Cam, Kustom Signals, Lenexa, KS
Motor Eye, Kustom Signals, Lenexa, KS
Cruise Cam, The Cruisers Division, Mamaroneck, NY
I Track, McCoy's Law Line, Chanute, KS
Docucam, MPH Industries Inc., Owensboro, KY
Digital Mobile Witness, T.A.W. Security Concepts, Wheat Ridge, COCar Camera
AV360, A.S.S.I.S.T. Internation- al, New York, NY
OPV, On Patrol Video, Ontario, OH
Gemini System, Decatur Electronics, Decatur, IL
SVS-500, ID Control Inc., Derry, NH
PAVE System, Video Systems Plus, Bryan, TX
InCharge 5555, Applied Integration, Tucson, AZ
VMDT, Coban Research and Technology, Houston, TX
Mobile Vision 5-C Video Recording System, Mobile Vision, Boonton, NJ
Stalker Vision VHS, Applied Concepts Inc., Plano, TX
Stalker Vision HI8, Applied Concepts Inc., Plano, TX
Digital Eyewitness, Kustom Signals, Lenexa, KS
Eagleye Model 800, Eagleye Technologies, Inc., Rome, GA
Eagleye Model 900, Eagleye Technologies, Inc., Rome, GA
Flashback, Mobile Vision, Inc., Boonton, NJ
Digital Patroller, Integrian, Morrisville, NC
Digital Patroller 2 Mobile Video Recorder, Digital Safety Technologies, Morrisville, NC
Panasonic Arbitrator 360 Mobile Video Recorder, Panasonic Corporation of North America, Secaucus, NJ
WatchGuard DV-1 Mobile Video Recorder, WatchGuard Video, Plano, TX EDGE Mobile Video Recorder, Coban Technologies, Stafford, TX
DVM-500 Plus and DVM-750 Mobile Video Recorders, Digital Ally, Overland Park, KS
WatchGuard 4RE Mobile Video Recorder, WatchGuard, Plano, TX
DigitalPatroller 3 Mobile Video Recorder, Digital Safety Technologies, Morrisville, NC
X22 Mobile Video Recorder, RDR Mobility, Flemington, NJ
Data 911 Mobile Digital Video System, Data 911 Mobile, Computer Systems, Alameda, CA
DVM-400 Mobile Video Recorder, Digital Ally, Lenexa, KS
DVB-777 Mobile Video Recorder, Digital Ally, Lenexa, KS

MVX1000 Mobile Video Recorder, Motorola Solutions Inc., Schaumburg, IL
DVM800, Digital Ally, Lenexa, KS
DVR-704, PRO-VISION, Byron Center, MI
1200-PA SD2+2, 10-8 Digital Video Evidence Solutions, Fayetteville, TN

Non-Vehicle-Mounted Mobile Video Recording Systems Overview

Non-Vehicle-Mounted Mobile Video Recording Systems shall be defined as those which are not permanently mounted in vehicles requiring the operator to possess a Class A, B, C or M Pennsylvania Driver's License, as defined in 75 Pa.C.S. § 1504. Non-vehicle-mounted mobile video recording systems shall include, but not be limited to, mobile video recorders worn on or about a law enforcement officer's person or affixed to an all-terrain vehicle, bicycle or horse.

The design of the non-vehicle-mounted mobile video recording system must use technology which includes a camera with date/time stamp capability, a microphone and a recording device, enclosed in secure protective enclosure(s). It may also contain controls, a monitor, GPS, wireless transceiver components and other electronic components. The non-vehicle-mounted mobile video recording system must be powered from a battery internal to the protective enclosure and must be weatherproof. The internal battery may be integral to the unit or removable. It is permissible to have an external battery to extend the operating life of the system. The non-vehicle-mounted mobile video recording system must have a minimum record time of 2 continuous hours. The system must operate over the following temperature range: -4°F to 122°F (-20°C to 50°C).

Camera

The camera component must have the following features:

A. Must be color video.

B. Minimum of 640 x 480 pixel resolution.

C. Minimum of 68 degrees field of view.

D. Minimum of 30 frames per second.

E. Minimum sensitivity rating of 3.4 lux or lower. Unit may use Infrared LED illumination to obtain lower than 3.4 lux equivalent.

F. Camera does not have to be in the same enclosure as the recorder. Can be connected to the recorder either by cable or wireless connection.

Recorder

The recorder component must have the following features:

A. Enclosed in a secure housing protected from physical damage.

B. Date/time recording index.

C. Minimum of 4 gigabytes of nonremovable solid state memory, 4 gigabytes

removable media or a combination of both removable and nonremovable memory.

D. Editing and record-over protection.

System Control

The system must:

A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.

B. Provide the user with the capability to manually turn the power on and off as necessary.

Wireless Link (optional)

The unit may use a wireless link to connect the camera to the recorder, recorder to another device, combination camera/recorder to another device or be used to download the evidence. The wireless link must have the following features:

A. Use a secure digital connection.

B. Wireless link can be used to play back a locally stored event on the recorder or store the media to a remote location such as secure Cloud storage.

C. FCC Type acceptable under 47 CFR Part 15 (relating to radio frequency devices).

The State Police, under the authority of 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4), has approved for use, until the next comprehensive list is published, subject to interim amendment, the following list of approved non-vehicle-mounted mobile video recording systems which meet the minimum equipment standards in this notice.

AXON Body Mobile Video Recorder, TASER, Scottsdale, AZ
AXON Flex Mobile Video Recorder, TASER, Scottsdale, AZ
FIRST Vu, Digital Ally, Lenexa, KS
FIRST Vu HD, Digital Ally, Lenexa, KS
LE 3 Mobile Video Recorder, VIEVU, Seattle, WA
BODYCAM BC-100, PRO-VISION, Byron Center, MI
Prima Facie, Safety Vision LLC, Houston, TX

Conducted Electrical Weapons with integrated Mobile Video Recording Systems

Notwithstanding any other standards or requirements contained in this notice, conducted electrical weapons equipped with integrated mobile video recording systems are only required to meet the following minimum specifications:

A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.

B. Be capable of having the audio video recording extracted from the conducted electrical weapon by means of downloading or by the removal of a media storage device.

Nothing in this notice prohibits the authorized use of a mobile video recording system that is not specifically identified if the mobile video recording system otherwise meets the equipment standards in this notice. Moreover, mobile video recording systems that are not activated to record oral communications or do not have an oral recording capability need not meet the equipment standards in this notice. Manufacturers may submit equipment to be added to the list by contacting the State Police, Bureau of Patrol (Bureau). New units must be in full commercial production. No prototype models will be considered. Proof of current sales and delivery of the specified equipment over the past 6 months must be provided, in writing, referencing current customers with contacts and phone numbers for verification. When requested by the Bureau, the manufacturer/bidder must furnish a complete working system installed in a vehicle for inspection within 30 days.

Comments, suggestions or questions should be directed to the State Police, Bureau of Patrol, Department Headquarters, 1800 Elmerton Avenue, Harrisburg, PA 17110.

COLONEL TYREE C. BLOCKER,
Acting Commissioner

[Pa.B. Doc. No. 15-1613. Filed for public inspection August 28, 2015, 9:00 a.m.]

NOTICES

STATE POLICE

Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems

[45 Pa.B. 5772]
[Saturday, September 19, 2015]

The State Police, under 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4) (relating to exceptions to prohibition of interception and disclosure of communications; and exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), published at 45 Pa.B. 5482 (August 29, 2015) a notice of Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems for use until the next comprehensive list is published.

As an addendum to the listing of approved mobile video recording systems published at 45 Pa.B. 5482, the State Police, under the authority cited previously, has approved for use, until the next comprehensive list is published, subject to interim amendment, the following additional mobile video recording system, which meets the minimum equipment standards published at 45 Pa.B. 5482:

Non-Vehicle-Mounted Mobile Video Recording System:

VISTA, Watchguard Video, Allen, TX

Comments, suggestions or questions should be directed to the State Police, Bureau of Patrol, Department Headquarters, 1800 Elmerton Avenue, Harrisburg, PA 17110.

COLONEL TYREE C. BLOCKER,
Acting Commissioner

[Pa.B. Doc. No. 15-1718. Filed for public inspection September 18, 2015, 9:00 a.m.]

NOTICES

STATE POLICE

Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems

[46 Pa.B. 116]
[Saturday, January 2, 2016]

The State Police, under 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4) (relating to exceptions to prohibition of interception and disclosure of communications; and exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), published at 45 Pa.B. 5482 (August 29, 2015) a notice of Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems for use until the next comprehensive list is published.

As an addendum to the listing of approved mobile video recording systems published at 45 Pa.B. 5482, the State Police, under the authority cited previously, has approved for use, until the next comprehensive list is published, subject to interim amendment, the following additional mobile video recording systems, which meet the minimum equipment standards published at 45 Pa.B. 5482:

Non-Vehicle-Mounted Mobile Video Recording Systems:

CopTrax SmartGLASS, CopTrax, Plano, TX

WOLFCOM Vision, WOLFCOM Enterprises, Hollywood, CA

Comments, suggestions or questions should be directed to the State Police, Bureau of Patrol, Department Headquarters, 1800 Elmerton Avenue, Harrisburg, PA 17110.

COLONEL TYREE C. BLOCKER,
Commissioner

[Pa.B. Doc. No. 16-37. Filed for public inspection December 31, 2015, 9:00 a.m.]

NOTICES

STATE POLICE

Law Enforcement Officer Camera System Data Handling Requirements

[47 Pa.B. 7815]
[Saturday, December 23, 2017]

The State Police, under 18 Pa.C.S. § 5706(b)(4) and (5) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), publishes this notice of the minimum standards to comply with the Federal Bureau of Investigation (FBI), Criminal Justice Information Service (CJIS), Security Policy, Version 5.6 (CJIS Policy) and 18 Pa.C.S. §§ 9101—9183 (relating to Criminal History Record Information Act) (CHRIA).

Camera systems used by criminal justice agencies in accordance with paragraph (2) of the definition of "oral communication" in 18 Pa.C.S. § 5702 (relating to definitions) have a high probability of capturing criminal justice information (CJI) and personally identifiable information. For these reasons, audio or video data, or both, (herein called "data") captured by these camera systems are considered CJI and shall be handled in accordance with the CJIS Policy, CHRIA and Commonwealth Law Enforcement Assistance Network (CLEAN) regulations. *Reference*: CJIS Policy; 18 Pa.C.S. § 9106(b)(3) (relating to information in central repository or automated systems); and the CLEAN regulations, State Police, CLEAN Administrative Section.

Criminal justice agencies shall request approval from the State Police, CLEAN Administrative Section, prior to storing any data onsite or offsite. This approval will ensure compliance with CJIS Policy requirements and CHRIA. In accordance with 18 Pa.C.S. § 5706(b)(5), the following are the minimum requirements that must be met for any storage of an audio recording made in accordance with 18 Pa.C.S. § 5706(b)(4), or any accompanying video recording:

A. Camera system

1. While worn by the officer, a camera system shall be considered a physically secure location.

2. Upon removal from the officer's body, the camera system shall be maintained in a physically secure location in accordance with CJIS Policy standards.

3. If a camera system is located in a criminal justice conveyance, it shall be considered located in a physically secure location. If the camera or hard drive is removed from the criminal justice conveyance, it shall conform with the CJIS Policy. A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods. A physically secure location, as stated in section 5.9.1 of the CJIS Policy (relating to physically secure location) is as follows:

A physically secure location is a facility, a criminal justice conveyance, or an area, room or a group of rooms within a facility, with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control, State Identification Bureau control, FBI CJIS security addendum, or a combination thereof, and shall consist of the following:

a. Security perimeter—area that is posted, separated and secured.

b. Physical access authorizations—list of authorized personnel.

c. Physical access control—control all physical access points (AP).

d. Access control for transmission medium—control physical access to information systems, distribution and lines.

e. Access control for display medium—not visible to unauthorized personnel.

f. Monitoring physical access—monitor and respond to security incidents.

g. Visitor control—authenticate and escort visitors.

h. The agency shall authorize and control information system-related items entering and exiting the physically secure location (delivery and removal).

B. Data transfer or downloading the data

1. If accomplished through a wireless connection, agencies shall meet the CJIS Policy requirements, as stated in section 5.13.1.1 (relating to 802.11 wireless protocols).

Note: Wired Equivalent Privacy and Wi-Fi Protected Access cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for Federal Information Processing Standard (FIPS) 140-2 and may not be used.

2. Agencies shall implement the following controls for all agency-managed wireless APs with access to an agency's network that processes unencrypted CJI:

a. Perform validation testing to ensure rogue APs do not exist in the 802.11 wireless local area network and to fully understand the wireless network security posture.

b. Maintain a complete inventory of all APs and 802.11 wireless devices.

c. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

d. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.

e. Enable user authentication and encryption mechanisms for the management interface of the AP.

f. Ensure that all APs have strong administrative passwords and ensure all passwords are changed in accordance with section 5.6.2.1 of the CJIS Policy (relating to standard authenticators), as follows:

(1) Be a minimum length of eight characters on all systems.

(2) Not be a dictionary word or proper name.

(3) Not be the same as the user ID.

(4) Expire within a maximum of 90 calendar days.

(5) Not be identical to the previous ten passwords.

(6) Not be transmitted in the clear, outside the secure location.

(7) Not be displayed when entered.

g. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

h. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, and the like) or services.

i. Enable all security features of the wireless product, including the cryptographic authentication, firewall and other available privacy features.

j. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.

k. Ensure that the ad-hoc mode has been disabled.

l. Disable all nonessential management protocols on the APs.

m. Ensure all management access and authentication occurs through FIPS-compliant secure protocols (for example, SFTP, HTTPS, SNMP over TLS, and the like). Disable non-FIPS-compliant secure access to the management interface.

n. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.

o. Insulate, virtually (for example, virtual local area network and access control lists) or physically (for example, firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.

p. When disposing of APs that will no longer be used by the agency, clear AP configuration to prevent disclosure of network configuration, keys, passwords, and the like.

3. If the data is manually downloaded by an individual or retained outside of a physically secure location, it will need to be encrypted at rest and in transit, per sections 5.10.1.2.1 and 5.10.1.2.2 of the CJIS Policy (relating to encryption for CJI in transit; and encryption for CJI at rest).

C. Storage of the data

Storage of data on location, if considered a physically secure location, shall be treated the same as all CJI at the location. Storage offsite, or in the cloud, shall meet all the requirements of the CJIS Policy for encryption while in transit and at rest, if applicable. If encryption is not used at rest, any person with access to the data or systems storing the data shall be properly vetted with a fingerprint-based background check and Security Awareness Training, and required agreements shall be maintained.

1. As stated in section 5.10.1.2.1 of the CJIS Policy:

> When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

2. As stated in section 5.10.1.2.2 of the CJIS Policy:

> When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

D. Reviewing and release of data

1. Data from the camera system shall only be reviewed by authorized personnel; that is, personnel that have been cleared through a fingerprint-based background check, have received Security Awareness Training and have signed the appropriate agreements, if applicable. If required, the Management Control Agreement for local government IT, or The Security Addendum for private contractors, shall be completed and on file.

2. Prior to the release of data from the camera system, the data shall be reviewed and any areas containing CJI shall be removed or rendered unintelligible. Any data received from CLEAN or the National Crime Information Center in either video or audio format, or both, shall be removed or rendered unintelligible prior to release to any unauthorized or unintended personnel.

E. Retention of data

Data shall be stored for 60 days unless needed for prosecution, courts, litigation, appeals or other operational needs.

F. Destruction of data

The data, or the data storage devices that are to be destroyed, shall be destroyed in compliance with the CJIS Policy, and a written destruction procedure that complies with the CJIS Policy shall be maintained at the agency. As stated in section 5.8.3 of the CJIS Policy (relating to digital media sanitization and disposal):

> The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

COLONEL TYREE C. BLOCKER,
Commissioner

[Pa.B. Doc. No. 17-2155. Filed for public inspection December 22, 2017, 9:00 a.m.]

PCCD Policy

These policy recommendations have been adopted by the Pennsylvania Commission on Crime and Delinquency (PCCD) in accordance with §67A07 of the Act 22 of 2017, which requires PCCD to condition grant funding related to body worn cameras (BWCs) on the following:

(b) The Pennsylvania Commission on Crime and Delinquency is authorized to condition funding or a grant related to the implementation, use, maintenance or storage of body worn cameras or recordings from body worn cameras on the following:

> **(b)(1) Requiring the grantee to have a protocol, guidelines or written policies related to the implementation, use, maintenance or storage of body worn cameras.**

> **(b)(2) Requiring that such a protocol, guidelines or written policies are publicly accessible, including being retrievable on a municipal website.**

(b)(3) Ensuring that the protocol, guidelines, or written policies substantially comply with applicable recommendations by the Commission.

According to these provisions, in order to be eligible for BWC related grant funding, agencies must issue a written, publicly accessible policy prior to implementing a BWC program that meets or exceeds these policy recommendations. Each of these agencies shall make a reasonable effort to comply with these recommendations. In some cases, agencies are at liberty to meet the policy recommendations in a manner that best suits their unique local needs and organizational structure.

PCCD strongly encourages agencies to develop their BWC policies and protocols in accordance with best practices with input from their Criminal Justice Advisory Board (CJAB) and community stakeholders, such as local victim service providers, community police review boards, and other interested parties.

The Body-Worn Camera Policy and Implementation Program (BWC PIP) aims to support the implementation of body-worn camera programs in law enforcement agencies across the country. The BWC PIP addresses the development and implementation of policies and practices for effective program adoption, and includes factors such as the purchase, deployment, and maintenance of camera systems and equipment; data storage and access; and privacy considerations. While BWC equipment may be purchased, award recipients must first demonstrate a commitment and adherence to a strong BWC policy framework, including comprehensive policy adoption and requisite training.
As a guideline, in months one through six of the grant, agencies will be expected to review and develop policies and training programs. As every agency faces different challenges and applicable laws, BJA will not set standards for policies and procedures. Policies must conform to applicable federal, state, local, and tribal laws. The Training and Technical Assistance (TTA) provider will work with the agency to document and validate the policy development process. The TTA provider must make recommendations to BJA that an agency has met the policy development requirements before BJA releases any award funds to the agency prior to implementation. During months seven through twenty-four, the grantees will be expected to deploy BWCs, continue their training efforts, and collect outcome measures to assess their BWC implementation.

Agencies are required to work with the BJA-funded BWC training and technical assistance (TTA) provider as part of the policy development process prior to the release of funds for implementation. Agencies must demonstrate appropriate policy development and internal law enforcement adoption prior to full funding being released by BJA for BWC procurement and implementation. Please note that PCCD funding is reimbursable (funds must be obligated or expended prior to PCCD's release of funds). Please use the following link for more information on
TTA: http://www.bwctta.com/training-and-technical-assistance