PENNSYLVANIA STATE POLICE
PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER

PRIVACY POLICY

I. Elements of Enabling Legislation or Authorization

A. Statement of Purpose

The purpose of this policy is to establish privacy guidelines for the Pennsylvania Criminal Intelligence Center (PaCIC). The mission of PaCIC is to support the decision-making process of Pennsylvania's law enforcement agencies through collating, analyzing, and disseminating intelligence and investigative information pertaining to criminal and terrorism activity while ensuring the rights and privacy of citizens.

B. Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

All PaCIC personnel will comply with this policy and 18 Pa C.S. §9106 (refer to Section IV. (1)) and the applicable laws as referenced in Section II. C. of this policy, protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. Federal regulation 28 CFR Part 23 (refer to Section IV. (2)) shall be adhered to in the situations wherein it is applicable.

It is PaCIC internal operating policy to comply with applicable laws as referenced in Section II. C. of this policy, protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system. All information provided by PaCIC from outside sources must be verified from those sources if the information is to be used in an investigative capacity.

All participating agency personnel, personnel providing information technology services to PaCIC, private contractors, governmental agencies including Information Sharing Environment (ISE) participating agencies and centers, and users will comply with this policy and with the applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies including ISE participating agencies and centers, and participating justice and public safety agencies, as well as private contractors, private entities, and the general public. Agencies receiving protected information as defined in 18 Pa C.S. §9106 must submit appropriate policies and procedures for dissemination of protected information.

C. Transparency and Accountability

PaCIC was created in July 2003 and was announced to the public in an August 2003 press statement issued by Governor Edward G. Rendell, Pennsylvania State Police (PSP) Commissioner Jeffrey B. Miller, and Pennsylvania Commission on Crime and Delinquency Chairman Jim Eisenhower. The policies on protection of privacy, civil rights, and civil liberties are available to the public on the Pennsylvania State Police Web site at www.psp.state.pa.us.

PaCIC personnel will follow 18 Pa C.S. §9106, directives and regulations issued by the Commissioner of the Pennsylvania State Police, and other laws as enacted by the Pennsylvania Legislature and signed by the Governor pertaining to the collection, collation, use, analysis, retention, destruction, sharing, and disclosure of intelligence information, archived information, and investigative information. PaCIC has established guidelines for accountability and compliance with all applicable laws and policies.

II. Elements of a Basic Internal Operations Policy

A. Definitions

Definitions contained in subsequent provisions of this policy which are applicable to specific provisions of this part, the following words, acronyms, and phrases when used in this policy shall have, unless the context clearly indicates otherwise, the meanings given to them in this Part:

Authorized User refers to an individual employed by the Pennsylvania State Police who is trained in the use of intelligence systems and has been provided appropriate access.

Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR) is a SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence information is information concerning the habits, practices, characteristics, possessions, associations, or financial status of any individual compiled in an effort to anticipate, prevent, monitor, investigate, or prosecute criminal activity.

Investigative information is information assembled as a result of the performance of any inquiry, formal or informal, into a criminal incident or an allegation of criminal wrongdoing and may include modus operandi information.

Law as used in this policy includes any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order.

Need to Know applies when as a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Pennsylvania Criminal Intelligence Center (PaCIC) is a component of the Pennsylvania State Police (PSP) that is staffed by PSP personnel as well as personnel from other law enforcement agencies. PaCIC is operational 24 hours a day, seven days a week to provide local, state, and federal law enforcement agencies access to publicly archived information, investigative information, and intelligence information.

Personal data refers to any personally identifiable information that relates to an identifiable individual.

Protected Information includes Personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Pennsylvania constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state constitutions; and applicable state, local, and ordinances. Protection may also be extended to organizations by center policy or state or local laws.

Public includes: (a) any person and any for-profit or nonprofit entity, organization, or association; (b) any governmental entity for which there is no existing specific law authorizing access to PSP information; (c) media organizations; and (d) entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from PSP.

Public does not include: (a) employees of PSP; (b) people or entities, private or governmental, who assist PSP in the operation of the justice information system; and (c) public agencies whose authority to access information gathered and retained by PSP is specified in law.

Qualified Individual is a person who has received appropriate training and has been provided necessary access in order to perform their duties.

Right to Know is based on having legal authority or responsibility or when, pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Role Based Access is a type of access authorization that uses roles to determine access rights and privileges.

Suspicious Activity Report (SAR) is the official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for feeding information repositories of data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

B. Seeking and Retaining Information

PSP will seek or retain only information concerning an individual or group reasonably suspected of criminal activity where such criminal activity would give rise to prosecution for a state offense graded a misdemeanor or felony or for a federal offense for which a penalty is imprisonment for more than one year, the source of the information is reliable and verifiable, or limitations on the quality of the information are identified. No information will be gathered or collected by PSP in violation of federal or state law.

PSP will not seek or retain and information-originating agencies will agree not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

The center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

PSP will adhere to the following practices regarding the receipt, collection, assessment, storage, access, dissemination, and retention of tips, leads, and suspicious incident reports: (a) the information received is assessed upon receipt for sensitivity and confidence and is treated appropriately; (b) the information is evaluated and investigated by trained personnel to determine its credibility, value, and appropriate categorization; (c) the information is stored and maintained in a secure environment with limited access and is labeled to delineate it from other information; (d) the information is only accessible to, and may be disseminated by, authorized personnel using the methods that apply to information that rises to the reasonable suspicion criteria; and (e) the information will be retained using the PSP retention schedule.

PSP will keep a record of the source of all information sought and collected by the center.

C. Methods of Seeking or Receiving Information

Information gathering and investigative techniques used by PSP will comply with the applicable federal and state laws and constitutional guarantees protecting the privacy, civil rights, and liberties of citizens. These include the Bill of Rights (the first 10 amendments to the U.S. Constitution), the Declaration of Rights to the Pennsylvania Constitution, the Pennsylvania Human Relations Act, the federal Civil Rights Act, 18 Pa C.S. §9106, 28 CFR Part 23 regarding criminal intelligence information, the OECD Fair Information Principles, and the criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan*.

In addition, policies regarding appropriate investigative techniques to be followed by PSP regarding the collection of information have been established through department issued operations manuals, administrative regulations, and field regulations.

PSP will not directly or indirectly receive, seek, accept, or retain information from an individual who may or may not receive a fee or benefit for providing the information, if PSP knows or has reason to believe that: (a) the individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to PSP; (b) the individual or information provider used methods for collecting the information that PSP itself could not legally use; (c) the specific information sought from the individual or information provider could not legally be collected by PSP; or (d) PSP has not taken the steps necessary to be authorized to collect the information. Non-government information providers under contract to provide information will have demonstrated they have appropriate safeguards and privacy policies in place.

D. Classification of Information Regarding Validity and Reliability

At the time of retention in the system, the information will be categorized regarding the: (a) the type of information (tips/leads, SARs, criminal intelligence information, etc.); (b) nature of the source; (c) reliability of the source; and (d) sensitivity of the information. The categorization and labeling of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information or there is a change in the use of the information affecting access or disclosure limitations, and as per scheduled established retention reviews.

E. Classification of Information Regarding Limitations on Access and Disclosure

At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations as identified in 18 Pa C.S. §9106 and 28 CFR Part 23 on access and sensitivity of disclosure in order to: (a) protect confidential sources and police undercover techniques and methods; (b) not interfere with or compromise pending

criminal investigations; (c) protect an individual's right of privacy and civil rights; and (d) provide legally required protection based on the status of an individual as a juvenile not subject to 18 Pa C.S. § 9105.

PSP applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is protected information to include personal information on any individual [see Section II. A., Definitions], and, to the extent expressly provided in this policy, includes organizational entities.

- The information is subject to 18 Pa C.S. §9106 and 28 CFR Part 23 provisions restricting access, use, or disclosure.

PSP will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

The classification of existing information will be reevaluated whenever: (a) new information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or (b) there is a change in the use of the information affecting access or disclosure limitations.

Credentialed, role-base access criteria will be used to control: (a) what information a class of users can have access; (b) what information a class of users can add, change, delete, or print; and (c) to whom the information can be disclosed and under what circumstances.

PSP personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Personnel will:

Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful.

Use a standard reporting format and data collection codes for SAR information.

Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection

process, supporting documentation, and labeling of the data to delineate it from other information.

Allow access to or disseminate the information using the same access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

Retain information for up to two years in order to investigate a tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, no further action, assigned, ongoing, completed) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

Adhere to and follow PSP physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

PSP incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

PSP will identify and review protected information that may be accessed or disseminated by PSP prior to sharing that information through the Information Sharing Environment. Further, PSP will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

PSP requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include: The name of the

originating center, department or agency, component, and subcomponent; the name of the center's justice information system from which the information is disseminated; the date the information was collected and, where feasible, the date its accuracy was last verified; and the title and contact information for the person to whom questions regarding the information should be directed.

F. Information Quality

PSP will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [refer to Section IV. H., Merging Information from Different Sources] has been met. PSP will make every reasonable effort to ensure that information sought or retained is updated and verified before taking any enforcement action based upon the information taken. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

Originating agencies external to PSP are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

PSP will advise recipient agencies in writing when information previously provided to them is deleted or changed because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

PSP investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

PSP will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system. PSP will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be deleted from the system when the agency learns that: (a) the information is erroneous, misleading, obsolete, or otherwise unreliable; (b) the source of the information did not have authority to gather the information or to provide the information to the agency; or (c) the source of the information used prohibited means to gather the information.

PSP's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff

will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

PSP's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals or organizations involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

Information-gathering and investigative techniques used by PSP will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

PSP will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

G. Collation and Analysis of Information

Types of information available for analysis include investigative, intelligence, open source, and public records (see Section II. B.). Information will only be analyzed: (a) by qualified individuals (see Section II. A.); (b) to provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals, and organizations suspected of having engaged in or engaging in criminal, including terrorist, activities generally; and (c) to further crime and terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by PSP. PSP personnel will comply with laws regarding privacy, civil rights, and civil liberties as outlined in Section I. B.

The PSP requires that all appropriate written analytical products be reviewed and approved by the Privacy Officer or in the Privacy Officer's absence, by the Privacy Officer's designee, to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination by the center.

H. Merging of Information from Different Sources

Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifying information sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of a match. Partial matches of information will be accompanied by a clear statement that it has not been established that the information

relates to the same individual and if matched will contain a clear statement that it has been adequately established that the information relates to the same individual or organization. Criteria for determining matches may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

I. Sharing and Disclosure of Information

Information gathered or collected and records retained by PSP will only be accessed by or disclosed to persons within the criminal justice system, persons within the center or in other governmental agencies who are authorized to have access and receive protected information and only for legitimate law enforcement, public prosecution, or justice purposes and only in the performance of official duties in the accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information or received information retained by PSP and the nature of the information accessed will be kept by PSP.

Information gathered or collected and records retained by PSP may only be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law if: (a) the information is reliable as determined by an authorized intelligence officer; (b) the agency requesting the information is a criminal justice agency which has policies and procedures consistent with 18 Pa C.S. §9106; and (c) the information requested is in connection with the duties of the criminal justice agency and the request is based on specific identifying information. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of five years by the center.

Information gathered or collected and records retained by PSP may be accessed or disseminated to those individuals responsible for public protection, public safety or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property. An audit trail sufficient to allow the identification of each individual who

accessed information or received information retained by PSP and the nature of the information accessed will be kept by PSP.

Information possessed by PSP that is considered nonpublic records will only be disclosed to an individual as the result of the issuance of a proper Subpoena Duces Tecum or, if the subpoena is objected to, a subsequent court order. An audit trail sufficient to allow the identification of each individual who accessed information or received information retained by PSP and the nature of the information accessed will be kept by PSP.

There are several categories of records that will not be provided to the public:

Records required to be kept confidential by law that are exempted from disclosure requirements under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008 (refer to Section IV. (3));

Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010;

Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008. However, certain law enforcement records must be made available for inspection and copying under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008;

A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008. This includes a record maintained by an agency in connection with the military, homeland security, national defense, law enforcement or other public safety activity that if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity or a record that is designated classified by an appropriate federal or state military authority;

Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under 18 Pa C.S. §9106, be shared without permission; or

A violation of an authorized nondisclosure agreement under 18 Pa C.S. §9106.

PSP shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

PSP will adhere to the current version of the ISE–SAR Functional Standard for the reporting of suspicious activity in the ISE, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

Redress:
Upon submission of and approval of a Pennsylvania Right to Know Law Request and satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the PaCIC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

The existence, nonexistence, content, and source of the information will not be made available by the PSP to an individual when:

> Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008);
>
> Disclosure would endanger the health or safety of an individual, organization, or community (Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008);
>
> The information is in a criminal information system subject to 28 CFR Part 23 and 18 Pa C.S. §9106;
>
> The information source does not reside with PSP or PSP did not originate and does not have a right to disclose the information (18 Pa C.S. §9106).

If the information did not originate with PSP, the requestor will be referred to the originating agency, if appropriate or required, or PSP will notify the source agency of the request and its determination that disclosure by PSP or referral of PSP to the source agency was neither required nor appropriate under applicable law.

If an individual requests correction of information ***originating with PSP*** that has been disclosed, the center's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights

if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

The individual who has requested disclosure will be given reasons if disclosure or requests for corrections are denied by PSP. The individual will also be informed of the procedure for appeal per the Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008 when PSP has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (a) is exempt from disclosure, (b) has been or may be shared through the ISE, (1) is held by PSP and (2) allegedly has resulted in demonstrable harm to the complainant, PSP will inform the individual of the procedure for submitting and resolving such complaints. Complaints can be sent by mail to the center's Privacy Policy Committee at the following address: Pennsylvania State Police, Pennsylvania Criminal Intelligence Center, Attention: Analytical Intelligence Section Commander, 1800 Elmerton Avenue, Harrisburg, PA 17110. Complaints can also be received by the Privacy Policy Committee via telephone at (717) 772-4140. The Privacy Policy Committee will refer the complaint to the PSP Office of Chief Counsel where it will be reviewed. The committee will acknowledge the complaint and state that it will be reviewed but not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Policy Committee will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by PSP that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, PSP will not share the information until such time as the complaint has been resolved. A record will be kept by PSP of all complaints and the resulting action taken in response to the complaint.

To delineate protected information shared through the ISE from other data, PSP maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

J. Information Retention and Destruction

Criminal intelligence information and SARs retained by PSP will be reviewed for purging at least every five years. Other information and intelligence will be reviewed as established by 18 Pa C.S. §9106. When information has no further value or meets the criteria for removal under 18 Pa C.S. §9106 and 28 CFR Part 23 (for criminal intelligence information), it will be purged, destroyed, deleted, or returned to the submitting source. Notification that information is subject to purging if not reviewed and verified will be provided at least 60 days prior to the required review and validation/purge date. A record shall be kept of when the information is to be reviewed for retention. The purging or removal of data shall be approved by a supervisor in accordance with applicable PSP administrative regulations.

According to 18 Pa C.S. §9106 and 28 CFR Part 23, as applicable, PSP will purge intelligence information under the following conditions: (a) the data is no longer relevant or necessary to the goals and objectives of the PSP; (b) the data has become obsolete, making it unreliable for present purposes and the utility of updating the data would be worthless, or (c) the data cannot be utilized for strategic or tactical intelligence studies.

K. Accountability and Enforcement

The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on the PSP public website at www.psp.state.pa.us.

PSP has established a Privacy Policy Committee which is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system; reports regarding alleged errors and violations of the provisions of this policy; receives and coordinates complaint resolution under the center's redress policy; and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. Committee members shall receive training in the protection of privacy, civil rights, and civil liberties. The committee's point of contact is the Analytical Intelligence Section Commander, who can be contacted by phone at (717) 772-4140, who will be trained and designated to serve as the Privacy Officer. Additionally external inquiries and complaints can be directed to the committee through the PSP Public Information Office. The Public Information Office can be contacted by phone at (717) 783-5556. Any complaints or reports of violations of department policies by PSP personnel will be handled through appropriate internal PSP policies and procedures. Inquiries or complaints that are received by the committee involving non-PSP personnel will be directed to the Analytical Intelligence Section Commander who will report the matter to the employee's agency. Information received by the PSP Public Information Officer pertaining to civil rights or civil liberties, will be immediately forwarded to the Privacy Committee for consideration.

Primary responsibility for the operation of this justice information system, including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy is assigned to the Director of the Pennsylvania State Police, Bureau of Criminal Investigation.

A supervisor within PaCIC designated as the security officer is responsible for handling any errors or violations with regard to this policy. The security officer shall receive appropriate training regarding the safeguarding and security of information. The security officer shall report all errors or violations of this policy to the Privacy Committee and the Analytical Intelligence Section Commander. The Analytical Intelligence Section Commander will ensure that enforcement procedures and sanctions outlined within this Part are adequate and enforced.

PSP has established procedures, practices, and system protocols and uses software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall comply with security requirements outlined in 18 Pa C.S. §9106.

PSP will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23 and 18 Pa C.S. §9106.

PSP will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions as provided in PSP regulations.

Queries made to PSP's data applications are logged into the data system identifying the user initiating the query. PSP will utilize watch logs to maintain audit trails of requested and disseminated information.

To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

PSP will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be conducted by PaCIC staff under the direction of the privacy officer, mandated at least annually, and a record of the audits will be maintained by the security officer of PaCIC.

PSP will periodically conduct audits and inspections of the information contained in the justice information system. The audits will be conducted randomly by a designated representative of PSP or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of information.

PSP will require any individuals authorized to use the system to acknowledge receipt of the policy and agree to comply with the provisions of this policy in writing. A copy of the policy, in a printed format, will be made available to all individuals authorized to use the system.

PSP reserves the right to restrict the qualifications and number of personnel having access to PaCIC information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating PaCIC's privacy policy.

The Privacy Policy Committee will annually review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations. This document can be altered and expanded as the ISE and other sharing systems are defined and implemented.

If a user is suspected of or found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, PSP will: (a) suspend or discontinue access to information by the user; (b) suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies; (c) apply other sanctions or administrative actions as provided in agency personnel policies; (d) request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or (e) refer the matter to appropriate authorities for criminal prosecution, as necessary.

In compliance with Pennsylvania's Breach of Personal Information Notification Act, PSP will notify individuals if their personal information is compromised by a breach of computer security unless it is determined that such notification would impede a criminal or civil investigation.

L. Training

PSP will require the following individuals to participate in introductory, and thereafter, annual training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy: (a) authorized users; (b) staff in other public agencies or private contractors providing services to PaCIC; and (c) users of the information system who are not employed by PSP.

The training program will cover: (a) any applicable federal or state statute, or any PSP regulation concerning privacy, civil rights, and civil liberties protection; (b) substance and intent of the provisions of the policy relating to collecting, use, analysis, retention, destruction, sharing, and disclosure of information retained by PSP; (c) the impact of improper activities associated with information accessible within or through the agency; (d) the nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any; and (e) PSP's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the ISE.

III. Sharing of Information among Participants

A. Expectations Regarding Information Gathered and Shared

Participating agencies, are governed by the laws and rules governing those individual agencies including applicable federal and state laws, with a memorandum of understanding or policies and procedures will adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to: (a) only seek or retain information that is legally permissible for the agency to seek or retain under laws applicable to the agency; (b) only use lawful means to seek information; (c) only seek and retain information that is reliably accurate, current, and complete, including the complete, relevant context; (d) take appropriate steps when merging information about an individual or organization from two or more sources to ensure that the information is about the same individual or organization and is referenced as to the source; (e) investigate in a timely manner any alleged errors and correct or delete information found to be erroneous; (f) retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to known or suspected criminal, including terrorist, activities; (g) maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions; (h) engage in collation and analysis of information in a manner that conforms to generally accepted practices; (i) establish procedures that comply with the policies and procedures of the justice information sharing system for accessing information through the participating agency; (j) only allow authorized users to access the information in the shared system and only for purposes related to the performance of their official duties; (k) share information with authorized users of other justice system partners based only on a "right-to-know" and a "need-to-know" basis; and (l) establish and comply with information retention and destruction schedules.

Information obtained from PSP will not be used or publicly disclosed for purposes other that those specified in the memorandum of understanding. Information cannot be sold, published, exchanged, or disclosed for commercial purposes; disclosed or published without prior approval of the contributing agency; or disseminated to unauthorized persons.

B. Use and Disclosure of Information Originating from another Participating Agency

A participating agency will not disclose information originating from another agency except as authorized or required by law in the jurisdiction in which the information originated or by following the third party dissemination rule, in which agencies external to PaCIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information as defined by 18 Pa C.S. §9106 and 28 CFR Part 23.

When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated in writing to the person designated in the originating agency to receive such alleged errors.

IV. Policy Attachments

(1) Title 18, Pa C.S. §9106
http://www.legis.state.pa.us/WU01/LI/LI/CT/HTM/18/00.091.006.000..HTM

(2) 28 CFR Part 23
https://www.dced.state.pa.us/public/oor/pa_righttoknowlaw.pdf

(3) Commonwealth of Pennsylvania Right to Know Law Act 3 of 2008
http://www.iir.com/Justice_Training/28cfr/guideline1.aspx