

ILLINOIS STATE POLICE DIRECTIVE
ADM-022, PRIVACY OF PERSONALLY IDENTIFYING INFORMATION

RESCINDS: ADM-022, 2012-057, REVISED 08-22-2012.	REVISED: 10-24-2017 2017-061
RELATED DOCUMENTS: None	RELATED CALEA STANDARDS: 42.1.6, 82.01.01, 82.01.03, 82.01.04, 82.01.06

I. POLICY

The Illinois State Police (ISP) will ensure the privacy and secure collection, maintenance, analysis, use and dissemination of personally identifying information.

II. AUTHORITY

- II.A. 28 Code of Federal Regulations (“CFR”) Part 23, “Criminal Intelligence Systems Operating Policies”
- II.B. Public Law 108–458, “Intelligence Reform and Terrorism Prevention Act of 2004”
- II.C. Civil Administrative Code of Illinois 20 ILCS 2605/2605-45(4) and 20 ILCS 2605/2605-500(3)
- II.D. Criminal Identification Act 20 ILCS 2630/
- II.E. Uniform Conviction Information Act 20 ILCS 2635/1
- II.F. Personal Identification Protection Act 815 ILCS 530/
- II.G. Identity Protection Act 5 ILCS 179/1
- II.H. Firearm Owners Identification Card Act 430 ILCS 65/
- II.I. Juvenile Court Act 705 ILCS 405
- II.J. FBI Criminal Justice Information Services Security Policy

III. DEFINITIONS

Personally Identifying Information - any data that can be used to uniquely identify, contact, or locate a single person or entity, including criminal justice information.

IV. RESPONSIBILITIES

The ISP Director will appoint an ISP Privacy Officer within the Director’s Office to oversee matters relating to the privacy of personally identifying information.

V. PROCEDURES

V.A. The Privacy Officer shall:

- V.A.1. Develop and revise policies and directives for ISP’s computerized records management systems. The Privacy Officer will work with various units within the Department to create policies designed to ensure that personally identifying electronic information, including intelligence information, owned or controlled by the ISP is collected, used, disseminated, and disposed of in an efficient and responsible manner.
- V.A.2. Have a thorough and comprehensive understanding of federal and state privacy laws and regulations and ensure ISP’s compliance with those laws and regulations.
- V.A.3. Identify the need for new or amended privacy laws and administrative rules regarding the protections of personally identifying information and propose appropriate changes.

- V.A.4. Ensure ISP's compliance with intelligence legislation, including but not limited to the Intelligence Reform and Terrorism Prevention Act of 2004 and 28 CFR Part 23, "Criminal Intelligence Systems Operating Policies."
- V.A.5. Understand the complex relationships between ISP and local/federal law enforcement agencies surrounding the compilation, utilization, and sharing of personally identifying electronic data.
- V.A.6. Seek input and feedback from other justice practitioners and relay those comments, where appropriate, to ISP Command.
- V.A.7. Work with other agencies/groups to develop memoranda of understanding (MOU) or agreements for ISP's computerized records management systems, specifically related to data privacy and information sharing. The Privacy Officer will implement and administer Information System Sharing Agreements/MOUs that foster the responsible exchange of criminal justice information between ISP and participating agencies.
- V.A.8. Represent the ISP's interests at privacy committees and associations as determined by the Director.
- V.A.9. Have access to classified intelligence data to assist work units with reviewing intelligence data in order to ensure compliance and train recipients of classified and sensitive information regarding its lawful collection, maintenance, analysis, use and dissemination.
- V.A.10. Review and approve all ISP Statewide Terrorism & Intelligence Center Threat Assessments prior to dissemination in a timely manner.
- V.A.11. Conduct an annual review of privacy policies, agreements, and MOUs and report any concerns to the Director and the ISP Chief Legal Officer.
- V.A.12. Be a licensed attorney authorized to practice in the State of Illinois.
- V.A.13. If possible, the Privacy Officer will be a Certified Information Privacy Professional with the International Association of Privacy Professionals.
- V.B. ISP employees who administer databases that collect and maintain personally identifying information will submit for review all policies governing the collection, maintenance, dissemination, and retention of that information through the Privacy Officer, prior to implementation of the database.
- V.C. ISP employees who enter into agreements or MOUs related to intelligence data, personally identifying information, or other privacy related issues shall provide a copy of such agreements or MOUs to the Privacy Officer for review no later than June 1st of each year.
- V.D. The ISP Governmental Affairs Office shall forward to the Privacy Officer for comment any proposed legislation that relates to the collection, maintenance, dissemination, and retention of personally identifying information.

| Indicates new or revised items.

-End of Directive-