

The Pegasus Program Privacy Policy

Pegasus Research Foundation
44 Avignon Ct. - Suite 100
Little Rock, AR 72223-9104

July 31, 2004

SECTION 1: PURPOSE

Programs, U.S. Department of Justice, has provided initial and follow-on funding for a pilot project entitled the Pegasus Multi-State System for Sharing Local Law Enforcement Information. The National Sheriffs' Association (NSA) and the Pegasus Research Foundation (PRF) initiated that pilot project. The Pegasus Program (sometimes referred to below as "Pegasus" or the "Program") grew from that project, which was initiated in response to the increased need for timely information sharing and exchange of information among members of the law enforcement community. PRF administers the Pegasus Program, including the communications and information technology system provided by the Program (the "Pegasus System"), and the Pegasus Advisory Board provides policy guidance for the Pegasus Program. The Pegasus Advisory Board is presently composed of seven Sheriffs from 5 states and an ex-officio member, the Executive Director of the NSA.

This Privacy Policy sets forth the Pegasus Program's policies regarding data privacy and protection of Pegasus Law Enforcement Information and other information contained in the Pegasus System, applicable to all Pegasus Participating Agencies and Pegasus Authorized Users. PRF may amend this Privacy Policy from time to time, in consultation with the Pegasus Advisory Board.

INFORMATION SHARING SERVICES FOR HOMELAND SECURITY

As part of the Nation's Homeland Security response to natural and man-made disasters and threats, the Pegasus Program, through the Pegasus System, provides a variety of information sharing services, which have value for both law enforcement and non-law enforcement Pegasus Program Agencies and individual Authorized Users. For example, the Agency Directory contains critical contact and other information (such as agency addresses, and telephone and fax numbers and email addresses for key agency personnel) for a wide range of law enforcement and non-law enforcement agencies, which the Pegasus Program intends to make available to Pegasus Authorized Users from both law enforcement and non-law enforcement agencies.

The Pegasus Program provides access to Pegasus Law Enforcement Information (as defined below) only to Pegasus Authorized Law Enforcement Users, which are designated by a Pegasus Law Enforcement Participating Agency.

"POINTER SYSTEM" FOR LAW ENFORCEMENT INFORMATION

The Pegasus Program is built upon law enforcement's experience that the timely exchange of accurate information can save countless investigative hours and significantly improve the opportunity for successful conclusion of investigations. The Program provides Pegasus Authorized Law Enforcement Users with access to Automated Data Exchange services utilizing a "pointer" system for Authorized Law Enforcement Users to locate and exchange existing non-intelligence law enforcement investigative and operational data from contributing law enforcement agency records management and jail management systems ("Law Enforcement Information"). The Pegasus System is not a "Criminal Intelligence System" as defined by 28 CFR Part 23, and it is the responsibility of each Pegasus Participating Agency to assure that the The Pegasus Program Privacy Law Enforcement Information it contributes is not "Criminal Intelligence Information", as defined by 28 CFR Part 23.

SECTION 2: COLLECTION AND CONTRIBUTION LIMITATIONS

The Pegasus Program operates for the purpose of sharing information by Pegasus Participating Agencies. The Pegasus System presents to Pegasus Authorized Law Enforcement Users an index of "pointer-type" Law Enforcement Information extracted from original source data contributed by law enforcement agencies with authority of the contributing agency. The Pegasus System currently extracts and maintains a copy of a sub-set of contributing agency original source data; the Program is also in discussion with some agencies, which wish to provide access to their original source data through a procedure under which the Pegasus

System does not maintain a copy of any original source data. Pegasus Participating Agency decisions to participate in the Pegasus Program, and to provide access to their databases, and how to do so, are voluntary and are governed by the laws of the respective states respecting such data, as well as by applicable federal law.

Because the laws, rules, or policies governing information that can be collected and released about individuals varies from state to state, limitations on the collection and contribution of data concerning individuals is the responsibility of the Pegasus Participating Agency which contributes the data to the Program. Each contributor of information to the Program undertakes to abide by the data collection and contribution limitations applicable to it due to law, rule, or policy. Pegasus Participating Agencies undertake to contribute to the Program only data, which has been collected and contributed in conformance with those limitations.

SECTION 3: LAW ENFORCEMENT INFORMATION QUALITY

Pegasus Participating Agencies remain the owners of the Law Enforcement Information they contribute and are, therefore, responsible for the quality and accuracy of the Law Enforcement Information accessed by Pegasus Authorized Law Enforcement Users.

Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Pegasus Program. In order to maintain the integrity of the Program, any information obtained through the Pegasus System must be independently verified by the Authorized User with the original data source before any official action (e.g., warrant or arrest) is taken. Pegasus Participating Agencies and individual Authorized Law Enforcement Users are responsible for compliance with Pegasus Privacy Policy and other policies of the Program in effect from time to time.

SECTION 4: USE LIMITATION

Law Enforcement Information obtained from or through the Pegasus Program (e.g., information from records management and jail management systems) may only be used by Authorized Law Enforcement Users for official law enforcement investigative purposes. An official law enforcement investigative purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation and operational case or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

Any non-Law Enforcement Information obtained from or through the Pegasus Program (e.g., Agency Directory information) may only be used by Authorized Users for official agency purposes. An official agency purpose means an official law enforcement investigative purpose or another operational purpose, which represents official business of the Pegasus Participating Agency, which employs the Authorized User.

PRF will take reasonable measures to secure access to the Pegasus System and prevent any unauthorized access or use of the Pegasus System. PRF reserves the right to restrict the qualifications and number of personnel who access the Pegasus System and to suspend or withhold service to any agency or individual violating this Privacy Policy. PRF further reserves the right to conduct inspections concerning the proper use and security of data accessible through the Pegasus System. Participating Agencies and Authorized Users are responsible for providing security for information derived from the Pegasus Program in accordance with applicable laws, rules, and regulations. Participating Agencies are also responsible for assuring that all personnel who receive, handle, or have access to Law Enforcement Information or other sensitive information are trained as to those requirements.

All individual Authorized Law Enforcement Users having access to the Pegasus System agree to abide by the following rules:

(a) Pegasus Law Enforcement Information will be used only to perform official law enforcement investigative-related duties in a manner authorized by the Authorized Law Enforcement User's agency.

- (b) The Pegasus System will be used only for official Participating Agency purposes in a manner authorized by the Authorized User's Participating Agency.
- (c) Individual passwords will not be disclosed to any other person except as authorized by Participating Agency management.
- (d) Individual passwords will be changed if authorized personnel of the Pegasus Participating Agency or PRF suspect the password has been improperly disclosed or otherwise compromised.
- (e) Pegasus Participating Agencies will authorize access to Law Enforcement Information only by Authorized Law Enforcement Users with completed background checks, unless waived on an individual basis by the Pegasus Participating Agency's senior executive.
- (f) Use of the Pegasus System in an unauthorized or illegal manner will subject the agency and/or user to denial of further use of the Pegasus System and Program, discipline by the user's employing agency, and/or criminal prosecution.
- (g) Every computer system has administrators who must have permission to access information in the system, in order to keep it operating. In addition to Pegasus System computer administrators who have undergone a background check and have agreed to abide by this Privacy Policy, senior representatives of the Authorized User's agency may monitor Authorized Users' use of the Pegasus System. Users of the Pegasus System are advised that their use of the Pegasus System may be monitored, and that users of the Pegasus System should have no expectation of privacy regarding their use or access of the Pegasus System.

Each Authorized User understands that access to the Pegasus System may be denied or rescinded for failure to comply with the applicable restrictions and use limitations and other Pegasus policies.

SECTION 5: SECURITY SAFEGUARDS

Information obtained from or through the Pegasus Program will not be used or publicly disclosed for purposes other than those specified in this Privacy Policy. Such information may not be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Pegasus Participating Agencies will authorize access to the Pegasus System only by individual Authorized Users who have been selected, approved, and trained accordingly. Pegasus Participating Agencies will authorize access to Pegasus Law Enforcement Information only by law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Pegasus Advisory Board. Each Participating Agency must complete a Consent and Release and Acknowledgment and Authorization prior to being provided access to the Pegasus System.

SECTION 6: OPENNESS

All Pegasus Participating Agencies will make this Privacy Policy available for public review or to any interested party. The Pegasus Program will post this Privacy Policy on its public Web site and make it available to any interested party.

SECTION 7: INDIVIDUAL PARTICIPATION

Law Enforcement Information presented in the Pegasus System is provided, on a voluntary basis, by Pegasus Participating Agencies and other contributing law enforcement agencies. Pegasus Law Enforcement Information and other data, information and services provided by the Pegasus System is made available "as-is" and is not represented or warranted as necessarily accurate, complete, or current except as verified by the original source. Each Authorized User remains solely responsible for the interpretation, further dissemination, and use of any information which results from use of the Pegasus System and is responsible for assuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public may not access individually identifiable information about themselves or others as users of the Pegasus System. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question. For example, each Pegasus Participating Agency must provide a means for an individual to review and challenge the accuracy and completeness of his or her criminal history record, as authorized and required by 28 CFR Section 20.21(g).

SECTION 8: ACCOUNTABILITY

When a Law Enforcement Information Automated Data Exchange query is made to the Pegasus System, the Pegasus System on the Authorized User's computer displays Law Enforcement Information. When such Law Enforcement Information is to be disseminated by an Authorized User to any person or agency other than the Authorized User's Participating Agency or the contributing agency which provided the original source data, the Participating Agency and the Authorized Law Enforcement User are responsible for maintaining a secondary dissemination log, in order to correct possible erroneous information and for audit purposes, as required by this Privacy Policy and any applicable law. Secondary dissemination of Law Enforcement Information may only be made to a law enforcement agency for an official law enforcement investigative purpose. Secondary dissemination of non-Law Enforcement Information may only be made for official law enforcement-related duties of the Authorized User's Participating Agency.

The agency from which Law Enforcement Information is requested will maintain a record (log) of any secondary dissemination of information when it includes criminal history information, personal information obtained in connection with a motor vehicle record as defined in 18 U.S.C. Section 2721 (Driver's Privacy Protection Act), or any other data designated by the Pegasus Program in consultation with the Pegasus Advisory Board, for at least five years. Any such record will reflect as a minimum: (a) Date of release; (b) To whom the information relates; (c) To whom the information was released (including address and telephone number); (d) The State Identification (SID) and/or the FBI number(s) or other information that clearly identifies the data released; and (e) The purpose for which the information was requested. Original source data, provided by the originating agency—not secondary data provided by the Pegasus System—must be used for any official action. Any such records will be maintained for a minimum of five years for audit purposes to ensure compliance with this Privacy Policy and with other applicable laws, policies, and regulations.

Pegasus System requirements for the Automated Data Exchange Function are still in process, with additional data types currently being added and refined. As System requirements for accountability reports are defined by the Program over the coming months, currently available System reports and additional reports, including user accountability reports, will be refined and made available for review by the Pegasus Program and senior management of Pegasus Participating Agencies. PRF will conduct or coordinate audits and investigate misuse of the Pegasus System. All violations and/or exceptions shall be reported to the Pegasus Advisory Board. Individual Authorized Users of the Pegasus System remain responsible for their legal and appropriate use of information contained therein. Failure to abide by the restrictions and use limitations for the use of the Pegasus System may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each Authorized User and Pegasus Participating Agency is required to abide by this Privacy Policy in the use of information obtained by and through the Pegasus System.