PENNSYLVANIA STATE POLICE
BUREAU OF RESEARCH AND DEVELOPMENT
1800 ELMERTON AVENUE
HARRISBURG, PA 17110
PHONE: 717-783-5536
FAX: 717-772-1435

Mailing date: December 30, 2003

Stefan Presser, Esquire
Legal Director
American Civil Liberties Union Foundation of Pennsylvania
P.O. Box 1161
Philadelphia, PA 19105-1161

Re: Right-to-Know Law Request No. 2003-141.

Dear Mr. Presser:

This letter acknowledges receipt by the Pennsylvania State Police (PSP) of your written request for records under the Pennsylvania *Right-to-Know Law (RTKL), 65 P. S. §§ 66.1 et seq.* For purposes of § 66.3-3(c)(1) of the RTKL, the "record[s] requested" are those described in your request, which is attached to this letter.

Subject to certain enumerated exceptions, the RTKL provides that "public records" consist of the following two categories: 1) "[a]ny account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property," and 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1.

Please be advised that -- as of this date -- PSP has not disbursed nor received any funds to date for the Multistate Anti-Terrorism Information Exchange (MATRIX) project, nor entered into any contract to disburse or receive such funds. [1] PSP has received software from Seisint, Inc. to use the MATRIX system, but that software was free of charge to PSP. PSP has also received computer equipment to upgrade our connection to the Regional Information Sharing Systems (RISS) network-- which is a pre-existing computer network upon which our connection to the MATRIX database relies -- but that equipment was also free of charge to PSP. Therefore, PSP does not have any records that fall into the accounts/vouchers/contracts category of the definition of "public records." 65 P.S. § 66.1; North Hills News Record v. McCandless, 722 A.2d 1037, 1039 (Pa. 1999) ("[t]o constitute a public record, the material at issue must bear a sufficient connection to fiscally related accounts, vouchers or contracts").

Moreover, please be advised that PSP has made five (5) "minute[s], order[s]

[1] Lt. Colonel Ralph Periandi, Deputy Commissioner of Operations, has received reimbursement for personal expenses incurred to attend MATRIX meetings, however.

or decision[s]" concerning the MATRIX project to date:

- On October 7, 2002, PSP announced its commitment to participate in the MATRIX project. This decision was made by then Commissioner Paul Evanko, and communicated by then Major Ralph Periandi, Director, Bureau of Criminal Investigation, during the MATRIX organizational meeting at the International Association of Chiefs of Police meeting in Minneapolis, Minnesota. This decision is memorialized in the MATRIX meeting minutes for October 7, 2002, which are being provided in response to your request (without waiver of the objections expressed herein). Record "A". The only record reviewed by Commissioner Evanko prior to making this decision was an email message from Major Periandi dated September 27, 2002, which is also being provided in response to your request. Record "B".
- On or about March 13, 2003, PSP agreed to contribute criminal history record information to the Florida Department of Law Enforcement (FDLE) for use in the MATRIX project. This decision and all of its essential components are memorialized in a Memorandum of Understanding (MOU), which is being provided in response to your request. Record "C".
- On or about August 28, 2003, PSP agreed to assist the Pennsylvania Department of Transportation and Pennsylvania Department of Corrections in providing certain additional data to FDLE for use in the MATRIX project. This decision and all of its essential components are memorialized in a MOU which is being provided in response to your request. Record "D".
- On or about November 12, 2003, certain PSP personnel decided to abide by certain security restrictions in order to become authorized users of the MATRIX system. This decision and all of its essential components are memorialized in the MATRIX User Agreement Form, which is being provided in response to your request. Record "E".
- On November 17, 2003, PSP agreed to abide by certain security restrictions so that its personnel could use the MATRIX system. This decision and all of its essential components are memorialized in the MATRIX Agency Security Agreement, which is being provided in response to your request. Record "F".

PSP's responses to your individual requests appear below. For purposes of clarity, I have numbered the individual requests contained in your letter.

#1. Denied. Requested records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, materials that are responsive to this request are not "records" of

PSP. Id. Rather, those materials are records of Seisint, Inc. and the MATRIX consortium, and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint protected by statute. 65 P.S. § 66.1. Without waiver of these objections, an informational brochure authorized for dissemination to the general public is being provided in response to your request. Record "G". Moreover, an informational website has been established to advise the general public about the MATRIX project, which is located at www.iir.com.

#2. Denied. Requested records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, materials that are responsive to this request are not "records" of PSP. Id. Rather, those materials are records of Seisint, Inc. and the MATRIX consortium, and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint protected by statute. 65 P.S. § 66.1. Without waiver of these objections, agreements and/or contracts signed by PSP to contribute data to the MATRIX project are being provided in response to your request. Records "C" – "F". Moreover, an informational brochure authorized for dissemination to the general public is being provided in response to your request. Record "G". Moreover, an informational website has been established to advise the general public about the MATRIX project, which is located at www.iir.com.

#3. No information responsive to request.

#4. No information responsive to request.

#5. DENIED. PSP has records identifying personnel with authorized access to MATRIX, but has no other information responsive to this request. PSP records containing the names of its personnel with authorized access to MATRIX are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, disclosure of the identities of PSP personnel with authorized access to MATRIX would operate to the impairment of a person's personal security. 65 P.S. § 66.1.

#6. Denied. Requested records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute,

order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, materials that are responsive to this request are not "records" of PSP. Id. Rather, those materials are records of Seisint, Inc. and the MATRIX consortium, and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint protected by statute. 65 P.S. § 66.1. Without waiver of these objections, agreements and/or contracts signed by PSP which contain procedures to protect individual privacy are being provided in response to your request. Records "C" – "F". Moreover, an informational brochure authorized for dissemination to the general public is being provided in response to your request. Record "G". Moreover, an informational website has been established to advise the general public about the MATRIX project, which is located at www.iir.com. Moreover, the MATRIX Privacy Policy authorized for dissemination to the general public is being provided in response to your request. Record "H". This policy is currently under review and subject to change.

#7. Denied in part. (i) PSP has documents describing the procedures for use of the MATRIX system. However, these records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, materials that are responsive to this request are not "records" of PSP. Id. Rather, those materials are records of Seisint, Inc. and the MATRIX consortium, and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint protected by statute. 65 P.S. § 66.1. Without waiver of these objections, agreements and/or contracts signed by PSP which contain procedures for use of the MATRIX system are being provided in response to your request. Records "C" – "F". (ii) PSP has documents containing usage statistics (as of week ending 10/24/2003) from Seisint Inc. However, these records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, materials that are responsive to this request are not "records" of PSP. Id. Rather, those materials are records of Seisint, Inc. and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint. 65 P.S. § 66.1. (iii) PSP is in possession of a document entitled Factual Analysis Criminal Threat Solution (FACTS) Success Stories dated October 2003. (The FACTS application is being used in the MATRIX project). However, this document is not a "public record" under the RTKL because it does not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies,

materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, this document is not a "record" of PSP. Id. Rather, this document is a record of FDLE, and is not maintained or controlled by PSP. Moreover, publication of this document would disclose the institution, progress or result of an investigation. Id. (iv) PSP has no other information responsive to this request.

#8. Denied. Requested records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, requested records constitute attorney-work product and are protected from disclosure by the attorney work product doctrine and the attorney-client privilege. 65 P.S. § 66.1; 42 Pa.C.S. § 5928; Pa.R.Civ.P. 4003.3.

#9. Denied. Requested records are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, these materials are not "records" of PSP. Id. Rather, these materials are records of Seisint, Inc., the MATRIX consortium, and/or FDLE, and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint protected by statute. 65 P.S. § 66.1. Without waiver of these objections, an informational website has been established to advise the general public about the MATRIX project, which is located at www.iir.com.

#10. Denied in part. PSP has no information on the number of people who have been trained to use MATRIX to date. Training materials used to train PSP personnel are not "public records" under the RTKL because they do not constitute an "account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property" or 2) "any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons." 65 P.S. § 66.1. Moreover, training materials are not "records" of PSP. Id. Rather, those materials are records of Seisint, Inc. and are not maintained or controlled by PSP. Moreover, materials from Seisint, Inc., contain the proprietary trade secrets of Seisint protected by statute. 65 P.S. § 66.1. A copy of the Individual User Agreement, signed by all MATRIX trainees from PSP, is being provided in response to your request. Record "F". PSP has no other information responsive to your request.

Right to Appeal

YOU HAVE A RIGHT TO CHALLENGE THIS DENIAL OF YOUR REQUEST. IN ORDER TO DO SO, YOU MUST FILE WRITTEN "EXCEPTIONS" TO THE RIGHT TO KNOW LAW EXCEPTIONS UNIT FOR THIS AGENCY WITHIN FIFTEEN (15) BUSINESS DAYS OF THE MAILING DATE OF THIS LETTER. YOUR WRITTEN EXCEPTIONS MUST STATE THE REASONS WHY YOU CLAIM THAT EACH IDENTIFIED RECORD IS A PUBLIC RECORD FOR PURPOSES OF THE RIGHT-TO-KNOW ACT. YOUR WRITTEN EXCEPTIONS ALSO MUST EXPLAIN WHY YOU DISAGREE WITH THE REASONS SET FORTH IN THIS LETTER FOR DENYING YOUR REQUEST. YOUR APPEAL MUST BE ADDRESSED TO THE FOLLOWING OFFICE:

Pennsylvania State Police
Bureau of Research and Development
ATTN: Right-to-Know Law Exceptions Official
1800 Elmerton Avenue
Harrisburg, PA 17110

Sincerely,

Cpl. William J. McAreavy 17098

Corporal William J. McAreavy
Right-to-Know Law Official/Liaison

ACLU Foundation of Pennsylvania
P.O. Box 1161
Philadelphia, PA 19105-1161
(215) 592-1513
fax: (215) 592-1343
info@aclupa.org

2003-0121

BY FAX AND FIRST CLASS MAIL

October 30, 2003

Pennsylvania State Police
Department Headquarters
Bureau of Research and Development
1800 Elmerton Avenue
Harrisburg, PA 17110
ATTN: Supervisor, Policies and Procedures Section

Re: Chapter 119 Public Records Request

To Whom It May Concern:

This is a formal request pursuant to 65 PS § 66.1-66.9, on behalf of the undersigned, to allow inspection and copying of the following public records,[1] including, but not limited to letters, correspondence, tape recordings, notes, data, memoranda, reports, email, computer source and object code, technical manuals, technical specifications, or any other materials, held by the Pennsylvania State Police Department regarding the Multistate Anti-Terrorism Information Exchange (MATRIX).

This request includes, but is not limited to records regarding:

1 • The specifications for the MATRIX, including, but not limited to documents regarding storage capacities, throughput (e.g. number of identity files processed per hour), types of computers used, and user manuals;

2 • What personal data is accessed and/or used by the MATRIX, including, but not limited to documents regarding the types of personal data (including, but not limited to drivers' records, financial records, medical information, marriage

[1] The term "record(s)" as used herein shall mean "all documents, papers, letters, maps, books, tapes, photographs, films, recordings or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

records, divorce records, Internet usage information, phone records, travel records, voting records, biometric data, educational records, information regarding race, ethnicity, immigration records, criminal justice records and/or gun owners' records) accessed or used by the MATRIX, the contents of any personal information databases related to the MATRIX, the number of individuals whose personal data has been obtained, how that data was obtained, including, but not limited to documents regarding how such data was selected for use in the MATRIX and any agreements and/or contracts to obtain such personal data, including, but not limited to any agreements and/or contracts with Seisint Inc. (Seisint).

3 • Any procedures for analyzing the data, including, but not limited to the criteria used by the MATRIX to determine whether someone is a terrorist, including, but not limited to the use of information regarding race, ethnicity, religious background, internet usage, travel patterns, political views, political activities and/or consumer purchasing habits in any way, shape or form;

4 • The results of any tests, including, but not limited to any logs or other written descriptions of how any such systems is and/or has been used, the accuracy rates of any such systems while in operation and assessments of the individuals whose data was collected and used;

5 • Who has access to the MATRIX, including, but not limited a complete list of all recipients of data from the MATRIX; any procedures for individuals to find out what information the MATRIX has about them, any procedures for individuals to correct information that the MATRIX has about them, and any procedures for individuals to find out what the MATRIX has determined about them;

6 • Any procedures in place to protect the privacy of the individuals whose data was accessed and/or used by the MATRIX, including, but not limited to documents regarding oversight boards, login restrictions, pop-up screens at sign-on, data security measures, encryption, reduced use of certain criteria (e.g. race and/or ethnicity) and/or data checking to ensure accuracy of the information, how any of the personal data accessed and/or used by the MATRIX will be destroyed, and documentation of any policies permitting such destruction;

7 • Details regarding usage of the MATRIX, including, but not limited to the number of times has the MATRIX been used, the cases or circumstances in which the MATRIX has been used (including, but not limited to instances where the MATRIX was used for non-terrorism investigations purposes and/or for non-criminal investigations purposes), the information that was collected in each instance, the results in instances when the MATRIX was used, including, but not limited to whether any terrorists were caught through use of the MATRIX in each instances, how many innocent people were caught through use of the MATRIX in each instance, notes or logs created during any of these instances where the MATRIX was used, and what happened to people identified by the MATRIX as a threat, the number of times the MATRIX has malfunctioned, the cases or circumstances in which the MATRIX malfunctioned, and what happened in each instance that the MATRIX malfunctioned, any procedures are in place for use/testing of the MATRIX, including, but not limited to who decides whether the MATRIX will be used/tested in a given case, procedures for handling requests to

use the MATRIX in a given case (including, but not limited to requests from state agencies, Federal agencies and/or private entities), the number of requests to use the MATRIX that have been received so far, the entities and/or individuals who have made requests to use the MATRIX, and the number of such requests that have been rejected,

8 • Any legal analyses regarding the MATRIX, including, but not limited to documents regarding whether the MATRIX violates international, federal, state and/or local privacy laws, including constitutional protections;

9 • Organizational details regarding the development and use of the MATRIX, including, but not limited to documents regarding sources of technical and/or financial support for the MATRIX, which federal, state and/or local government agencies are involved and/or cooperating in the MATRIX project, the extent to which such agencies are involved and/or cooperating in the MATRIX project, what companies (including, but not limited to Seisint), consultants and or colleges are involved and/or cooperating in the MATRIX project, the extent to which such companies, consultants and/or colleges are involved and/or cooperating in the MATRIX project, what companies, the amount of money spent on developing the MATRIX system so far, the sources for this money, and budgetary outlays for future development and/or maintenance of the MATRIX; and,

10 • Records regarding training of people to use the MATRIX, including, but not limited to textbooks, video presentations, contracts and/or agreements to be signed by MATRIX trainees, and the number of people who have been trained to use the MATRIX so far.

This request also includes, but is not restricted to information regarding similar activities being conducted by any public and/or private agency or organization.

Pennsylvania's Public Records Law expresses the state's policy that all state records be available at all times for inspection by any person. In accordance with 65 PS § 66.1-66.9, we would like the requested records to be made available to us immediately. If, for any reason, any of the requested records will not be made available to us immediately, please advise us in writing as soon as possible at fax number (215) 592-1343.

Pursuant to 65 PS § 66.1-66.9 further provides that if the person who has custody of a public record contends that the record or part of it is exempt from inspection, such person must state the basis for the exemption which the person contends is applicable to the record, including the statutory citation to an exemption created or afforded by statute. Additionally, if requested by the person who has custody of the public record must state in writing and with particularity the reasons for his conclusion that the record is exempt. We hereby request that any person claiming an exemption state in writing both the statutory citation for any exemption deemed applicable to any requested record and the specific reasons for a conclusion that any requested record is exempt.

Pennsylvania provides that a person who has custody of a public record and who asserts that an exemption applies to a particular public record or part of such record shall

delete or excise from the record only that portion of the record with respect to which an exemption has been asserted and validly applies, and such person shall produce the remainder of such record for inspection and examination.

Also, please note that Pennsylvania's Right to Know Law prohibits the destruction of any of the requested records, including any which you claim are exempt, for a period of 30 days after the date on which you receive this written request. If a civil action is instituted to enforce the Public Records Law with respect to the requested records within the 30-day period, you may not dispose of the records except by court order after notice to all affected parties.

As used herein, the term "relating to" is used in the broadest possible sense and means and includes: describing, explaining, analyzing, encompassing, including, containing, embodying, comprising, identifying, constituting, verifying, reflecting, referring to, containing reference to, contradicting, refuting, evidencing, dealing with, commenting on, responding to, supplementing, and/or supporting. The word "relating" is defined to include the common meaning of those terms, and shall include indirect as well as direct references to, description of or commentary on the subject matter set forth in this Request.

The word "documents" is used in the broadest possible sense, and means and includes all written, recorded, or graphic matters, however produced or reproduced, including computer files, tapes, disks or diskettes and computer generated reports, whether or not privileged, pertaining in any way to the subject matters of this Request. This definition includes, but is not limited to, any and all originals, copies, or drafts of any and all of the following which are in the possession, custody and control of any Department official, employee, agent or representative: records, notes, messages, phone messages, summaries, schedules, contracts or agreements; plans, drawings, maps, specifications, invoices, proposals, quotations, orders or acknowledgments; diaries or desk, pocket or other calendars; reports, forecasts, financing statements, instruments, financial statements, books of account, ledgers, journals, accounting or other work papers; charts, schedules, tabulations or appraisals; memorandum, letters, e-mails, telegrams, telexes, or cables prepared, drafted, received or sent; tapes, transcripts or recordings; photographs, pictures or films; or any other graphic recorded or written material of any nature whatsoever. "Document" shall be deemed to include any summary of a document of documents requested.

The word "communications" means any transfer of information regardless of means of communication, including but not limited to, those by oral, written, electronic, photographic or other means, and includes any record or memorialization of the communication by any means whatsoever.

Please be advised that this Public Records Request is intended to be as broad and inclusive as permitted by law and is intended to apply to all officers, officials, employees, departments, divisions, bureaus, commissions, councils, and any other private agency,

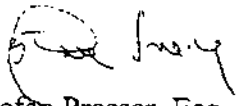
person, partnership, corporation or business entity acting on behalf of, or with the knowledge of, the Department.

In accordance with state law and in furtherance of compliance with our Public Records Request, we ask that the custodians of the records hereby requested make an investigation of this Request to ensure full compliance with all applicable provisions of 65 PS § 66.1-66.9.

We agree to compensate the Department for the cost of duplicating any of the records of which we request duplication, as provided by law. Upon locating the requested documents, please contact us prior to photocopying and advise us of the actual costs of duplication or any necessary staff research time so that we may decide whether a narrowing of the request will be necessary.

If you have any questions, please do not hesitate to contact us. Your immediate attention to these matters is greatly appreciated. Thank you for your assistance.

Sincerely,



Stefan Presser, Esq.
Legal Director

Multistate Anti-Terrorism Information Exchange (MATRIX) Meeting

October 7, 2002
Minneapolis, Minnesota

On Monday, October 7, 2002, the organizational meeting of the Multistate Anti-TeRrorism Information EXchange project (MATRIX) was held in Minneapolis, Minnesota. This was a follow-up to an earlier meeting held in Orlando, Florida, in March. Representatives from the states of California, Florida, Georgia, Iowa, Kentucky, Louisiana, Michigan, New York, Oregon, Pennsylvania, Texas, and Utah attended the meeting. The states of Ohio and South Carolina, also a part of this effort, were not represented.

Commissioner Tim Moore, Florida Department of Law Enforcement (FDLE), called the meeting to order and asked for introductions from attendees. The following were in attendance at the meeting.

Mr. Bob Cummings, Florida Department of Law Enforcement
Mr. Steven Cumoletti, New York State Police
Ms. Karen Halliday, Michigan State Police
Mr. Tim Hazlette, Kentucky State Police
Mr. Vernon Keenan, Georgia Bureau of Investigation
Mr. Pat Lunney, California Department of Justice
Mr. Stephen Madden, Michigan State Police
Mr. Kent Mawyer, Texas Department of Public Safety
Mr. Jeffrey Miller, Pennsylvania State Police
Mr. Peter Modafferi, Rockland County, New York, District Attorney's Office
Mr. Tim Moore, Florida Department of Law Enforcement
Mr. Michael Nagurny, Pennsylvania State Police
Mr. Ralph Periandi, Pennsylvania State Police
Mr. Russell Porter, Iowa Department of Public Safety
Mr. Jeff Portz, Florida Department of Law Enforcement
Mr. Phil Ramer, Florida Department of Law Enforcement
Mr. Ron Ruecker, Oregon State Police
Mr. Roland Squire, Utah Department of Public Safety
Mr. George Vinson, California Governor's Office
Mr. Verdi White, Utah Governor's Office
Mr. Jim Willis, Oregon State Police
Mr. Walter Wolfe, Louisiana State Police

The following individuals were also in attendance at the meeting.

Mr. Doug Bodrero, IIR
Mr. Paul Cameron, Seisint
Mr. Bill Eubanks, Federal Bureau of Investigation
Mr. Angelo Fiumara, RISS Office of Information Technology
Mr. Clay Jester, IIR
Mr. Dan Latham, Seisint

Mr. Zheng Liu, RISS Office of Information Technology
Mr. Jerry Lynch, MAGLOCLEN
Mr. George March, RISS Office of Information Technology
Ms. Angie McKenzie, IIR
Mr. Bill Shrewsberry, Seisint
Mr. Richard Ward, Bureau of Justice Assistance, DOJ
Mr. Emory Williams, IIR

The following MATRIX participants did not attend the meeting.

Mr. Ted Almay, Ohio Office of the Attorney General
Mr. Bob Bertee, Michigan State Police
Mr. Rodney Brewer, Kentucky State Police
Mr. Marshall Caskey, Texas Department of Public Safety
Mr. Jeff Mayberry, Kentucky State Police
Mr. Mark Oxley, Louisiana State Police
Mr. Robert Stewart, South Carolina Law Enforcement Division

Commissioner Moore provided background information regarding the MATRIX project and the purpose of the organizational meeting. Participants were advised that a grant proposal in the amount of $5 million has been submitted to the Bureau of Justice Assistance (BJA). The proposal was submitted by the Institute for Intergovernmental Research (IIR) pursuant to an earlier decision by the participating states and a Memorandum of Understanding previously signed by the states. Commissioner Moore stated that when the grant award is received, IIR will provide administration and coordination of the grant award for the MATRIX participants.

Mr. Emory Williams, IIR, provided a presentation that briefly described the MATRIX grant application. The grant provides for three major accomplishments: (1) establishment of a secure Web site in each state, (2) node connection to riss.net (or single connections of users if desired), and (3) expanding the FDLE data mining capability to other states. A breakdown was provided of the MATRIX budget. If the project is awarded at $4 million instead of $5 million, decisions would have to be made by the Executive Committee regarding budget cuts. Because all states may not need or want all of the items that are provided for in the grant, this permits some flexibility in use of the funds. A list of MATRIX resources was reviewed, including details of IIR's role in the project. Information on the Regional Information Sharing Systems (RISS)/Law Enforcement Online (LEO) interconnection and the RISS Anti-Terrorism Information Exchange (ATIX) was also provided. A proposed timeline for the grant award was reviewed.

According to provisions of the grant application, a Chairman and an Executive Committee needed to be elected. Commissioner Moore was nominated and elected unanimously by the participants as Chairman of the MATRIX Participant Group.

Chairman Moore advised that participants needed to elect states that would serve as members of the Executive Committee. Chairman Moore suggested that the states of California, Georgia, New York, Oregon, and Pennsylvania make up the Executive Committee. By a unanimous vote, these states were selected as members of the

Executive Committee, along with Florida (by virtue of Chairman Moore being from Florida).

Chairman Moore introduced Mr. Paul Cameron, CEO, Seisint. Mr. Cameron provided background information on Seisint. Seisint's data products include a multi-billion record repository of information on U.S. individuals and businesses. They provide a unique combination of data, association algorithms, and technologies that offer extremely rapid results. Their products are available through ready-to-use Web and client-based applications, batch processes, and XML-based system-to-system interfaces. Seisint has been in business for approximately four years and currently has 45,000 users per day. Mr. Cameron advised that after September 11, the company decided to focus some of its efforts on delivering information to law enforcement to assist in terrorism investigations. FDLE was subsequently contacted, and with the help of the FBI, INS, DEA, and the U.S. Secret Service, the FDLE data mining application, called FCIC Plus, was developed. Mr. Cameron advised that all FDLE security requirements were met, but additional security requirements could be added if required.

Mr. Cameron introduced Mr. Jeff Portz, FDLE, who provided a demonstration of the FCIC Plus application. FCIC Plus is the Seisint-produced data mining application. The MATRIX project will expand this capability to further develop and accommodate additional state participant needs. Consideration will be given to a name that better represents the constituency of the project. The application contains driver's license images, motor vehicle registrations, an electronic generated line-up capability, terrorism factor information query capability based on pre-established criteria to identify potential terrorist connections, historical and current information on addresses and telephone numbers, and mapping software. In response to a question about how often the driver's license and vehicle registration information is updated, Mr. Portz advised that the information is updated every month to a month and a half.

After the demonstration, discussions were held on the costs involved. Chairman Moore advised that once the grant award is received, some of the money will be used to offset the front-end cost. A pricing structure will then be provided to the states. Mr. Williams advised that an agreement would have to be developed between the group and Seisint detailing the costs and a billing structure.

Mr. Cameron pointed out that there would be a one-time charge to host the data, plus a cost per user. The cost would be based on the number of users. Chairman Moore advised that each of the states will need to provide information on the size and number of files and the number of users (both law enforcement and non law enforcement).

Chairman Moore began discussions of the other agenda items. The first item discussed was the states' commitment to participate in the MATRIX project. All participants present indicated their commitment to the project. Chairman Moore advised that Mr. Robert Stewart, South Carolina Law Enforcement Division, and Mr. Ted Almay, Ohio Office of the Attorney General, were not able to attend the meeting; however, Chairman Moore spoke with each of them to confirm their commitment to participate in

the project. Chairman Moore indicated that the Executive Committee and IIR will work with each participating state to determine their specific needs.

A discussion was held on the project organization and future meetings. Chairman Moore indicated that a listserv will be created. The listserv will be used to provide information electronically to participants. Chairman Moore suggested that the next meeting of all participants be held in the next 30-45 days. Mr. Williams pointed out that travel costs will need to be paid by the participants if the grant has not been awarded. The Executive Committee will meet to discuss a date for the meeting of all participants. At a minimum, a conference call can be scheduled.

A suggestion was made that each of the states be asked to identify who the contacts will be in each state, especially for technical matters.

Discussions were held on the type of data to include for data mining. The types of data suggested by the participants included criminal history, driver's licenses (including images), corrections data, and regulatory data. A question was asked regarding what public data Seisint has so that efforts are not duplicated. Mr. Cameron indicated that Seisint could provide the information. It was suggested that some states would prefer data access and security be controlled by FDLE rather than Seisint, as some states may not legally be able to place their data with a private company. A suggestion was made that subcommittees may be needed to look at specific issues. A question was raised about audit trails. Mr. Cameron indicated that every query is being logged.

Chairman Moore asked participants if law changes or executive orders would be needed to permit the states to add their data to the data-mining database. Several participants indicated they did not know what process would be used. Others indicated they would need to request legal opinions.

Additional funding sources for the project were discussed. Chairman Moore indicated that $10 million was the original amount needed for the initiation of the project; however, the grant award was submitted for $5 million because of funding limitations and may be reduced to $4 million at award time. This necessitates finding supplemental funding in the near future.

Mr. Williams advised the participants that a marketing package was needed to put in the hands of governors and other states that might have an interest in joining the project, assuming additional funding becomes available. The marketing package will be used to provide a full understanding of the project and needs to be developed quickly and in conjunction with the RISS ATIX marketing package that is currently under development by IIR.

It was asked if the regional RISS policy board would need to approve the states in their region before the states could become nodes on riss.net. Mr. Williams indicated that the states would need approval, and each RISS center director will be asked to expedite the process.

All participants unanimously selected MATRIX as the name of the project. A suggestion was made that the MATRIX presentation provided by IIR be e-mailed to all participants. Mr. Williams suggested that he would add one additional slide to the presentation that would include a summary of the meeting. IIR was asked to e-mail the presentation before the end of the week due to some participants having meetings the following week in their states.

Discussions were held regarding a second group of states being included in the project. Mr. Richard Ward, BJA, suggested that the group needed a proof of concept before the project be opened to other states. A suggestion was made that the participants identify states that are ready to come on board once the concept can be shown. The states could start working on items that will be needed to participate.

Additional discussions were held on the MATRIX marketing package. A suggestion was made that the marketing package include a reference to checks and balances on the use of data. Chairman Moore stated that no new data would be added.

Chairman Moore indicated that the Executive Committee would meet soon, and another meeting of the entire group would be scheduled in 30-45 days.

The meeting was adjourned.

Periandi, Ralph M

From: Periandi, Ralph M

Sent: Friday, September 27, 2002 10:08 AM

To: Evanko, Paul J; Werts, Robert G

Cc: Hickes, Robert C; Miller, Jeffrey B (PSP) (HARRISBURG); Waugh, Wesley R; Kurtz, Jon D; Young, David F (PSP) (HQ); Petyak, Ronald P

Subject: Twelve State National Information Sharing Initiative

Cols.,

The original ten state national initiative re: info. sharing (the previous mtg. I attended w/ Maj. Jeff Miller in Fla.) has expanded to include twelve states: California, Florida, Georgia, Kentucky, Louisiana, Michigan, New York, Ohio, Oregon, Pennsylvania, South Carolina, Texas. I participated in a conference call yesterday w/ reps. from each of the above listed states. Commissioner Tim Moore, Fla. Dept. of Law Enforcement has taken the lead in this initiative.

A $5 mil. Federal grant has been secured by IIR through BJA and Homeland Security. It will fund each state's connectivity to Riss.Net as a node (unk. if that is identical to our previous discussions w/ MAGLOCLEN), a webpage for each state to facilitate data mining, and 850 end user certificates per state.

The project has developed into two independent initiatives:

1. database dumps to a secure central file
2. intelligence pointer-index info. sharing

The requested database dumps include: criminal history, drivers license, vehicle registration, and corrections files. This info. would be secured with Accurint a trademark of Seisint, Boca Raton, Fla. (PSP observed a demo. of their capabilities previously in the High-Tech. Conf. Rm. facilitated by Accenture) and merged with their public records files.

Intelligence pointer-index info. would be posted by each agency on their respective webpages. We would have complete autonomy regarding what if any info. we post.

The initial project is the database dump. As you can see, this appears to be beyond the scope of the sole authority of PSP, and may become a J-Net issue as well. There are legal issues, policy guidelines, and tracking requirements to name just a few of the considerations needing to be addressed.

A mtg. has been scheduled on Monday, Oct. 7, from 1300 - 1600 hrs. in Minneapolis during the IACP Conference. I will attend and request that, at a minimum, Majors Jeff Miller and Wes Waugh accompany me due to their positions in PSP and likelihood they would be affected by any involvement we commence on this project. I need to submit the names of PSP mtg. attendees by Tue., Sept. 24.

The mtg. agenda includes:

1. an overview of the IIR/BJA Federal Funding Grant
2. a commitment from each state to participate
3. a list of databases which will be shared by a participating state
4. election of an executive board

I may have an opportunity to secure PSP a position on the executive board if you so desire. However, that would not be feasible if we (Pennsylvania) are not committed to the project. At a minimum we have the following issues to resolve:

1. connectivity to Riss.Net as a node (previously rejected - is this the same process?)
2. periodic database dumps from various files (legal, policy, tracking considerations)
3. security of Accurint files and security clearance of its management and personnel

I'm certain there are others concerns I have not immediately listed. Also, some of these issues may need to be clarified with and approved by the Gov's office.

I am requesting guidance as to how to proceed at the mtg. on Oct 7. If we are firmly committed, I can be as active a participant as you direct . On the other hand, I can take a more passive/tentative approach if we are undecided. I sense the grant funding will be distributed on a first come - first serve basis among committed participants.

Thanks, Rick.

MEMORANDUM OF UNDERSTANDING BETWEEN THE PENNSYLVANIA STATE POLICE AND THE FLORIDA DEPARTMENT OF LAW ENFORCEMENT FOR THE PURPOSE OF SHARING DATA TO BE SEARCHED AGAINST THE PROPRIETARY DATABASES OF SEISINT, INC.

This Memorandum of Understanding (hereinafter referred to as "MOU"), by and between the Pennsylvania State Police, (hereinafter "PSP"), 1800 Elmerton Avenue, Harrisburg, Pennsylvania, and the Florida Department of Law Enforcement (hereinafter "FDLE"), is for the purpose of setting out the terms and conditions under which PSP will share certain types of its data with FDLE, to allow searches involving such data against the proprietary databases of Seisint, Inc. (hereinafter "Seisint"), for criminal investigative and intelligence purposes.

1. The sharing and use of PSP's data by FDLE is for the public good, and each party to this MOU will be responsible for its own costs in implementing the MOU.

2. This MOU specifies the terms and conditions under which PSP's data will be transferred to FDLE to facilitate its search against information in the Seisint databases, but is limited to the purposes expressed herein and neither FDLE nor PSP shall be construed as the agent, servant, joint venturer, or partner of the other.

3. The references to the parties to this MOU shall, unless the context would not permit, be understood to include, but not be limited to, the parties' officers, agents, employees, contractors, assigns, and successors.

Description of Data Sharing

4. PSP will, at a time or times duly agreed upon by the parties, provide to FDLE's Office of Statewide Intelligence an electronic copy in a format agreed upon by the parties of the following databases which PSP maintains and has custody and control over as a part of its lawful duties and responsibilities: criminal history record information, as that term is defined under the Pennsylvania Criminal History Record Information Act (CHRIA), 18 Pa.C.S. § 9101 *et seq.*

5. The criminal history record information furnished by PSP pursuant to this MOU is made available to FDLE on the condition of and solely and exclusively for use in searching that information against other databases for criminal intelligence and investigative purposes, and thus after dissemination is considered part of a criminal intelligence and investigative database, as those terms are defined in Florida law, which is exempt from disclosure under Florida's public records laws (Chapter 119, Florida Statutes).

6. PSP acknowledges and agrees that FDLE is receiving the criminal history record information (data) specified above as-is, without review or inspection, and FDLE does not warrant or represent that said information is accurate, complete, or current.

7. PSP acknowledges that the process of utilizing its data against the information contained in Seisint's databases will involve comprehensively comparing and cross-referencing the former for any matches, similarities, or points of commonality with the latter, without limitation or restriction as to the kind or quantity of information thereby derived or produced and further acknowledges that the other parties to this cooperative effort will initiate searches upon its data for criminal investigative and intelligence efforts.

8. Each law enforcement agency utilizing the data searches described herein will be required to acknowledge that such agency remains solely responsible for the interpretation, further dissemination, and use of any information which results from the search process, and is responsible for assuring that any information relied upon is accurate, current, valid, and complete.

9. PSP will notify FDLE whenever data previously provided by PSP is subsequently expunged or corrected. FDLE will subsequently expunge the data in accordance with the expungement or correction order, and will provide any certification of the expungement or correction as may be required by PSP.

Security of Data

10. PSP's data which is transferred for use in searches against the Seisint database will be stored and maintained in a secure manner. An authorized FDLE representative(s) will be responsible to monitor, inspect, and control all operations regarding FDLE's use of PSP's data. PSP's data is subject to the terms and conditions of the Agreement which FDLE has entered into with Seisint for the security and protection of FDLE's data that is to be searched against Seisint's databases, and nothing herein limits the scope or extent of that agreement. FDLE will not use or attempt to use PSP's data or any information derived from or produced by the search process described above for any purpose other than legitimate criminal justice investigative and intelligence purposes, and will share any and all information derived from or produced by the search process described above with PSP upon PSP's request at no charge. FDLE will not otherwise acquire, capture, copy, modify, or release information or data derived indirectly or directly from PSP's data made available or from the search process described above. FDLE will not rescind, amend, or otherwise alter the terms and conditions contained in its Agreement with Seisint, dated October 12, 2001, without prior notice to PSP.

11. Each party to this MOU acknowledges and agrees that any material violation of the restrictions set forth in this MOU will be grounds for immediate termination of the offending agency in participation in the cooperative effort defined by this MOU. All parties acknowledge that any unauthorized or improper dissemination of submitted data or information derived from or produced by the search process described above could compromise criminal investigations and endanger the safety of individuals.

12. Upon termination, for any reason, of this MOU, any PSP data and any information derived from or produced by the search process described above which is

physically or electronically located in premises or equipment under FDLE's custody or control, will be promptly returned to PSP, or shall be physically destroyed in a manner acceptable to PSP, and monitored and verified in writing by FDLE, at PSP's option.

13. PSP shall have the right to stop, cancel, suspend, or otherwise limit access by FDLE or Seisint to its data and to any information derived from or produced by the search process described above at any time.

14. PSP understands and acknowledges that law enforcement agencies within Pennsylvania will have access to the contributed data via the Seisint search system and agrees to monitor and control such use to assure it is consistent with the purposes and limitations set forth herein.

General Terms and Conditions

15. The initial term of this MOU shall be through 2003, effective from the date of execution by authorized officers of each participating agency and FDLE. Renewal shall be automatic on a year-to-year basis, effective each January 1, until such time as the MOU is terminated in writing. This MOU is terminable by any party upon thirty days advance written notice provided to:

Executive Director
Florida Department of Law Enforcement
P.O. Box 1489
Tallahassee, Florida 32302-1489.

16. This MOU shall be construed in accordance with the laws of the State of Florida. The PSP's participation in and obligations under this MOU shall be governed by the laws of the Commonwealth of Pennsylvania.

17. No party to this MOU shall assign, sublicense nor otherwise transfer its rights, duties and/or obligation under this MOU without the prior written consent of the other parties, in which case any successor in interest shall assume all such rights, duties and/or obligations remaining under this MOU.

18. This MOU may not be amended except in writing, by mutual consent of the parties.

19. PSP acknowledges that FDLE may enter into agreements similar to this MOU with other entities which perform or assist in performing a criminal justice function.

20. FDLE shall not be considered to be a "repository" of Pennsylvania criminal history record information under Pennsylvania law.

21. FDLE acknowledges that the equipment utilized to store criminal history record information is solely dedicated to purposes related to the administration of

criminal justice, or, if the equipment is not used solely for the administration of criminal justice, FDLE is accorded equal management participation in computer operations used to store the criminal history record information.

22. FDLE acknowledges that it has instituted procedures to reasonably protect the equipment used to store criminal history record information from theft, fire, sabotage, flood, wind or other natural or man-made disasters.

23. FDLE acknowledges that its employees authorized to have access to criminal history record information have been selected, trained, and supervised by FDLE.

24. FDLE agrees that, if requested, the Pennsylvania Attorney General may conduct an audit of the criminal history record information provided to FDLE by PSP under this MOU.

IN WITNESS WHEREOF, FDLE AND PSP have caused this Memorandum of Understanding to be executed by their respective undersigned officials authorized to do so, effective upon the last date specified below.

For FDLE:

James T. Moore
Name

Commissioner
Title

3/30/03
Date

For PSP:

Jeffrey B. Miller
Name

Acting Commissioner
Title

03-13-03
Date

MEMORANDUM OF UNDERSTANDING BETWEEN THE FLORIDA DEPARTMENT OF LAW ENFORCEMENT AND THE PENNSYLVANIA STATE POLICE, PENNSYLVANIA DEPARTMENT OF TRANSPORTATION, AND PENNSYLVANIA DEPARTMENT OF CORRECTIONS FOR THE PURPOSE OF SHARING DATA TO BE SEARCHED AGAINST THE PROPRIETARY DATABASES OF SEISINT, INC.

This Memorandum of Understanding (hereinafter referred to as "MOU"), by and between the Florida Department of Law Enforcement (hereinafter "FDLE") and the Pennsylvania State Police, (hereinafter "PSP"), 1800 Elmerton Avenue, Harrisburg, PA 17110, the Pennsylvania Department of Transportation, (hereinafter "DOT"), 1101 South Front Street Harrisburg, PA 17104-2516, and the Pennsylvania Department of Corrections, (hereinafter "DOC"), P.O. Box 598, 2520 Lisburn Road, Camp Hill, PA 17011, is for the purpose of setting out the terms and conditions under which PSP, DOT, and DOC will share certain types of data with FDLE, to allow searches involving such data against the proprietary databases of Seisint, Inc. (hereinafter "Seisint"), for criminal investigative and intelligence purposes.

1. The sharing and use of PSP, DOT, and DOC data by FDLE is for the public good, and each party to this MOU will be responsible for its own costs in implementing the MOU.

2. This MOU specifies the terms and conditions under which PSP, DOT, and DOC data will be transferred to FDLE to facilitate its search against information in the Seisint databases, but is limited to the purposes expressed herein and neither FDLE nor PSP, DOT, or DOC shall be construed as the agent, servant, joint venturer, or partner of the other.

3. The references to the parties to this MOU shall, unless the context would not permit, be understood to include, but not be limited to, the parties' officers, agents, employees, contractors, assigns, and successors.

Description of Data Sharing -- PSP Data

4. PSP will, at a time or times duly agreed upon by the parties, provide to FDLE's Office of Statewide Intelligence an electronic copy (in a format agreed upon by the parties) of the following databases which PSP maintains and has custody and control over as a part of its lawful duties and responsibilities: criminal history record information, which is defined and regulated by the Pennsylvania Criminal History Record Information Act (CHRIA), 18 Pa.C.S. § 9101 *et seq.*

5. The data furnished by PSP pursuant to this MOU is made available to FDLE on the condition of and solely and exclusively for use in searching that information against other databases for criminal intelligence and investigative purposes, and thus after dissemination the data is considered part of a criminal intelligence and investigative

database, as those terms are defined in Florida law, which is exempt from disclosure under Florida's public records laws (Chapter 119, Florida Statutes).

6. PSP and FDLE acknowledge and agree that FDLE is receiving the criminal history record information (data) specified above as-is, without review or inspection, and PSP and FDLE do not warrant or represent that said information is accurate, complete, or current.

7. PSP acknowledges that the process of utilizing its data against the information contained in Seisint's databases will involve comprehensively comparing and cross-referencing the former for any matches, similarities, or points of commonality with the latter, without limitation or restriction as to the kind or quantity of information thereby derived or produced and further acknowledges that the other parties to this cooperative effort will initiate searches upon such data for criminal investigative and intelligence efforts.

8. Any law enforcement agency utilizing the data searches described herein will be required to acknowledge that such law enforcement agency remains solely responsible for the interpretation, further dissemination, and use of any information which results from the search process, and is responsible for assuring that any information relied upon is accurate, current, valid, and complete.

9. Pennsylvania criminal history record information that is corrected in or expunged from the central repository in accordance with CHRIA will be corrected or deleted and provided to FDLE on a scheduled basis. Upon request, FDLE will provide any certification of the correction or expungement as may be required by PSP.

10. FDLE shall not be considered to be a "repository" of Pennsylvania criminal history record information under Pennsylvania law.

11. FDLE acknowledges that the equipment utilized to store criminal history record information is solely dedicated to purposes related to the administration of criminal justice, or, if the equipment is not used solely for the administration of criminal justice, FDLE is accorded equal management participation in computer operations used to store the criminal history record information.

12. FDLE acknowledges that it has instituted procedures to reasonably protect the equipment used to store criminal history record information from theft, fire, sabotage, flood, wind or other natural or man-made disasters.

13. FDLE acknowledges that its employees authorized to have access to criminal history record information have been selected, trained, and supervised by FDLE.

14. FDLE agrees that, if requested, the Pennsylvania Attorney General may conduct an audit of the criminal history record information provided to FDLE by PSP under this MOU.

15. Upon termination for any reason of this MOU, any and all PSP data and any and all information derived from or produced by the search process described above which is physically or electronically located in premises or equipment under FDLE's custody or control will be promptly returned to PSP, or shall be physically destroyed in a manner acceptable to PSP, and monitored and verified in writing by FDLE, at PSP's option.

Description of Data Sharing -- DOC Data

16. DOC will, at a time or times duly agreed upon by the parties, provide PSP with an electronic copy in a format agreed upon by the parties of the following databases which DOC maintains and has custody and control over as a part of its lawful duties and responsibilities: (a) criminal history record information, which is defined and regulated by the Pennsylvania Criminal History Record Information Act (CHRIA), 18 Pa.C.S. § 9101 *et seq.*; (b) visitor tracking information; (c) inmate account information; and (d) inmate phone lists. PSP will subsequently provide this information to FDLE's Office of Statewide Intelligence.

17. DOC hereby acknowledges, pursuant to the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa.C.S. § 5704(13), that all inmates of its facilities have been notified that their telephone conversations may be intercepted, recorded, monitored, or divulged. Moreover, DOC acknowledges that it has promulgated guidelines to implement § 5704(13) for state correctional facilities.

18. The data furnished by DOC pursuant to this MOU is made available to FDLE on the condition of and solely and exclusively for use in searching that information against other databases for criminal intelligence and investigative purposes, and thus after dissemination is considered part of a criminal intelligence and investigative database, as those terms are defined in Florida law, which is exempt from disclosure under Florida's public records laws (Chapter 119, Florida Statutes).

19. DOC and FDLE acknowledge and agree that FDLE is receiving the data specified above as-is, without review or inspection, and DOC and FDLE do not warrant or represent that said information is accurate, complete, or current.

20. DOC acknowledges that the process of utilizing its data against the information contained in Seisint's databases will involve comprehensively comparing and cross-referencing the former for any matches, similarities, or points of commonality with the latter, without limitation or restriction as to the kind or quantity of information thereby derived or produced and further acknowledges that the other parties to this cooperative effort will initiate searches upon such data for criminal investigative and intelligence efforts.

21. Any law enforcement agency utilizing the data searches described herein will be required to acknowledge that such law enforcement agency remains solely

responsible for the interpretation, further dissemination, and use of any information which results from the search process, and is responsible for assuring that any information relied upon is accurate, current, valid, and complete.

22. DOC will notify PSP whenever criminal history record information previously provided by DOC is subsequently expunged or corrected. PSP will then provide this information to FDLE. Pennsylvania criminal history record information that is corrected or expunged in accordance with CHRIA will be corrected or deleted and provided to FDLE on a scheduled basis. Upon request, FDLE will provide any certification of the correction or expungement as may be required by DOC.

23. FDLE shall not be considered to be a "repository" of Pennsylvania criminal history record information under Pennsylvania law.

24. FDLE acknowledges that the equipment utilized to store criminal history record information is solely dedicated to purposes related to the administration of criminal justice, or, if the equipment is not used solely for the administration of criminal justice, FDLE is accorded equal management participation in computer operations used to store the criminal history record information.

25. FDLE acknowledges that it has instituted procedures to reasonably protect the equipment used to store criminal history record information from theft, fire, sabotage, flood, wind or other natural or man-made disasters.

26. FDLE acknowledges that its employees authorized to have access to criminal history record information have been selected, trained, and supervised by FDLE.

27. FDLE agrees that, if requested, the Pennsylvania Attorney General may conduct an audit of the criminal history record information provided to FDLE by DOC under this MOU.

28. Upon termination for any reason of this MOU, any and all DOC data which is physically or electronically located in premises or equipment under FDLE's custody or control will be promptly returned to DOC, or shall be physically destroyed in a manner acceptable to DOC, and monitored and verified in writing by FDLE, at DOC's option.

Description of Data Sharing -- DOT Data

29. DOT will, at a time or times duly agreed upon by the parties, provide to PSP an electronic copy in a format agreed upon by the parties of the following data which DOT maintains and has custody and control over as a part of its lawful duties and responsibilities -- motor vehicle and driver record information, which is defined and regulated by federal and Pennsylvania law. PSP will subsequently provide this information to FDLE's Office of Statewide Intelligence.

30. FDLE is a "law enforcement agency" under the Driver Privacy Protection Act, 18 U.S.C. § 2721, and FDLE requires the data to carry out its functions as the Security Agent for the Multistate AntiTerrorism Information Exchange (MATRIX) project.

31. FDLE is a "State . . . governmental agency" under the Pennsylvania Vehicle Code, 75 Pa.C.S. § 6114(b)(4), and FDLE requires the data for the sole purpose of exercising a legitimate governmental function or duty.

32. The data furnished by DOT pursuant to this MOU is made available to FDLE on the condition of and solely and exclusively for use in searching that information against other databases for criminal intelligence and investigative purposes, and thus after dissemination such data is considered part of a criminal intelligence and investigative database, as those terms are defined in Florida law, which is exempt from disclosure under Florida's public records laws (Chapter 119, Florida Statutes).

33. DOT and FDLE acknowledge and agree that FDLE is receiving the data as-is, without review or inspection, and DOT and FDLE do not warrant or represent that said information is accurate, complete, or current.

34. DOT acknowledges that the process of utilizing its data against the information contained in Seisint's databases will involve comprehensively comparing and cross-referencing the former for any matches, similarities, or points of commonality with the latter, without limitation or restriction as to the kind or quantity of information thereby derived or produced and further acknowledges that the other parties to this cooperative effort will initiate searches upon such data for criminal investigative and intelligence efforts.

35. Data supplied by DOT to FDLE shall only be utilized as set forth in this MOU, and such data may not be sold, published, or disclosed for any commercial purpose nor without prior DOT approval.

36. Each law enforcement agency utilizing the data searches described herein will be required to acknowledge that such law enforcement agency remains solely responsible for the interpretation, further dissemination, and use of any information which results from the search process, that any dissemination or use will be in accordance with this MOU, and that the law enforcement agency is responsible for assuring that any information relied upon is accurate, current, valid, and complete.

37. FDLE acknowledges that the equipment utilized to store the data is solely dedicated to purposes related to the administration of criminal justice, or, if the equipment is not used solely for the administration of criminal justice, FDLE is accorded equal management participation in computer operations used to store the criminal history record information.

38. FDLE acknowledges that it has instituted procedures to reasonably protect the equipment used to store the data from theft, fire, sabotage, flood, wind or other natural or man-made disasters.

39. FDLE acknowledges that its employees authorized to have access to the data have been selected, trained, and supervised by FDLE.

40. FDLE agrees that DOT, or an independent auditor selected by DOT, may audit the DOT data furnished to FDLE under this MOU. FDLE reserves the right to approve the independent auditor selected by DOT, and its approval will not be unreasonably withheld.

41. DOT retains exclusive ownership of its data supplied to FDLE under this MOU.

42. FDLE agrees that records must be kept for a period of five years identifying each person or entity that receives DOT data and the permitted purpose for which the data will be used and must make such records available to DOT upon request. Such records must include the name, address, and telephone number of the person or entity that receives the DOT data.

43. Upon termination for any reason of this MOU, any and all DOT data which is physically or electronically located in premises or equipment under FDLE's custody or control will be promptly returned to DOT, or shall be physically destroyed in a manner acceptable to DOT, and monitored and verified in writing by FDLE, at DOT's option.

Security of Data

44. PSP, DOC, and DOT data that is transferred for use in searches against the Seisint database will be stored and maintained in a secure manner. An authorized FDLE representative(s) will be responsible to monitor, inspect, and control all operations regarding FDLE's use of PSP, DOC, and DOT data. PSP, DOC, and DOT data is subject to the terms and conditions of the Agreement which FDLE has entered into with Seisint for the security and protection of FDLE's data that is to be searched against Seisint's databases, and nothing herein limits the scope or extent of that agreement. PSP, DOC, and DOT data will be considered "FDLE data" for purposes of the Agreement which FDLE has entered into with Seisint. FDLE will not use or attempt to use PSP, DOC, or DOT data or any information derived from or produced by the search process described above for any purpose other than legitimate criminal justice investigative and intelligence purposes, and will share any and all information derived from or produced by the search process described above with PSP upon PSP's request at no charge. FDLE will not otherwise acquire, capture, copy, modify, or release information or data derived indirectly or directly from the PSP, DOC, or DOT data made available from the search process described above. FDLE will not rescind or materially amend or alter the terms

and conditions contained in its Amended Memorandum of Understanding with Seisint, signed by FDLE on May 13, 2003, without prior notice to PSP, DOC, and DOT.

45. All law enforcement agencies that will have access to PSP, DOC, and DOT data shall be required to sign a written agreement that shall include a provision that states that the agency shall not sell, publish or disclose any of the data or portions thereof furnished to FDLE under this MOU for any commercial purpose, nor use any of the data obtained from the search process for any purpose other than for a legitimate criminal justice investigative or intelligence function.

46. Each party to this MOU acknowledges and agrees that any material violation of the restrictions set forth in this MOU will be grounds for immediate termination of the offending agency in participation in the cooperative effort defined by this MOU. All parties acknowledge that any unauthorized or improper dissemination of submitted data or information derived from or produced by the search process described above could compromise criminal investigations and endanger the safety of individuals.

47. PSP, DOC, and DOT shall have the right to stop, cancel, suspend, or otherwise limit access by FDLE or Seisint to its data and to any information derived from or produced by the search process described above at any time.

General Terms and Conditions

48. The initial term of this MOU shall be through 2003, effective from the date of execution by authorized officers of each participating agency and FDLE. Renewal shall be automatic on a year-to-year basis, effective each January 1, until such time as the MOU is terminated in writing. Any party may terminate its participation in this MOU upon thirty days advance written notice provided to:

Executive Director
Florida Department of Law Enforcement
P.O. Box 1489
Tallahassee, Florida 32302-1489

Deputy Commissioner of Operations
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110

Executive Deputy Secretary
Pennsylvania Department of Corrections
2520 Lisburn Road, Box 598
Camp Hill, PA 17001-0598

Deputy Secretary for Safety Admin.
Pennsylvania Dept. of Transportation
Riverfront Office Center, 4th Floor
1101 South Front Street
Harrisburg, PA 17104-2516

49. No party to this MOU shall assign, sublicense nor otherwise transfer its rights, duties and/or obligation under this MOU without the prior written consent of the other parties, in which case any successor in interest shall assume all such rights, duties and/or obligations remaining under this MOU.

50. This MOU may not be amended except in writing, by mutual consent of the parties.

51. PSP, DOC, and DOT acknowledge that FDLE may enter into agreements similar to this MOU with other entities which perform or assist in performing a criminal justice function.

52. PSP, DOT and DOC understand and acknowledge that law enforcement agencies within Pennsylvania will have access to the contributed data via the Seisint search system, and PSP agrees to monitor and control such use to assure it is consistent with the purposes and limitations set forth herein.

53. By entering into this MOU, none of the parties waive any defenses or immunities to which they are entitled under Florida and Pennsylvania law, as well as federal law.

IN WITNESS WHEREOF, FDLE AND PSP, DOC, and DOT have caused this Memorandum of Understanding to be executed by their respective undersigned officials authorized to do so, effective upon the last date specified below.

For FDLE:

Name

Commissioner
Title

11/5/03
Date

For PSP:

Col. Jeffrey B. Miller
Name

Commissioner
Title

08-28-03
Date

For DOC:

Name

Secretary
Title

9/29/03

For DOT:

Allen D. Biehler
Name

Secretary
Title

9/11/03

Multi-State Anti-Terrorism Information eXchange

User Agreement Form

(PLEASE TYPE OR PRINT CLEARLY, ALL FIELDS MUST BE COMPLETED)

Check Applications to Request Access:		☐ New Application ☐ Revision	
Applicant Information:		☐ Sworn ☐ Non-Sworn	
Name (Last, First, MI): State/NCIC Cert: Yes ☐ No ☐		Title/Rank:	ID #
Date of Birth: / /	Social Security #: - -	Sex: ☐ Male ☐ Female	Race:
E-Mail Address: (Must be a Secure Address)	Work Number: ( ) -	Fax Number: ( ) -	RISS User ID:

Applicant Agency Information:	
Agency Name:	Agency ORI:
Agency Mailing Address:	Applicant's Supervisor Name (Title/Rank):

Terms of Agreement:

In consideration for the privilege of access to the information in the MATRIX Applications, including but not limited to FCIC+, the individual User whose name and employing agency appear on this agreement, agrees to the following conditions:

1. The User acknowledges that the MATRIX Executive Policy Group shall not be liable for the use made of the MATRIX applications by the individual User or the consequences of that use, and that the User or User's employing agency, or both, remain responsible for the acts or omissions of such User in connection with access to and use of the information in FCIC+.
2. The User is aware that the information found in MATRIX Applications may contain errors. The User will not take action based solely on this information without independently verifying the validity and accuracy of that information.
3. **The User understands and accepts that any non-compliance with the terms of this Agreement or any unauthorized or improper use or dissemination of information derived from MATRIX applications may subject the User or the User's employing agency to discontinuance of service. Moreover, certain offenses against system security and the improper dissemination of the information contained therein are crimes under State and Federal law.**
4. The User agrees to abide by the following rules and understands that access to MATRIX applications is strictly conditioned upon such compliance:
   (a) Individual User codes will be used only for authorized law enforcement investigative or intelligence purposes and only in an official capacity.
   (b) Sensitive information (for example, made confidential or exempt from disclosure by law) will not be released or disseminated to any unauthorized person or entity.
   (c) Individual User passwords will not be disclosed to any other person except as expressly authorized by User's employing agency management.
   (d) Individual passwords will be changed if the User reasonably suspects that his or her password has been improperly disclosed or compromised.
   (e) Information will only be accessed or printed out for authorized law enforcement investigative or intelligence purposes and only in an official capacity.
   (f) A log of all criminal history record disseminations will be maintained.
5. The User acknowledges that the user is aware of and bound by the terms and conditions of the MATRIX Law Enforcement Agency Security Agreement entered into by the user's employing agency
6. **An applicant's background check shall consist of the following: a fingerprint based records check (from anytime during applicant's employment at the employing agency listed on this form), an intelligence file check and an active warrants check (local, state and federal). The background should be consistent with your state's requirement for Police Officers. The Supervisor's signature attests to the completed background.**

Acknowledgement of Agreement:			
Background Completed:	☐ Yes ☐ No	Background Satisfactory:	☐ Yes ☐ No
Applicant Signature	Date	Applicant Supervisor Signature (Same as Above)	Date
Official Use Only:			
Training Instructor:		Initials:	Date:
Approval/Authorization:		User ID:	Date:

EXHIBIT E

Effective Date: 08/2003

Revised: 08/2003

MATRIX
Agency Security Agreement

This agreement is entered into between the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the State of Florida with headquarters at 2331 Phillips Road, Tallahassee, Florida, as the designated Security Agent for the Multistate AntiTerrorism Information Exchange Project (hereinafter referred to as MATRIX) and the Pennsylvania State Police, with headquarters at 1800 Elmerton Avenue, Harrisburg, Pennsylvania 17110, hereinafter referred to as the Agency), for the purpose of providing access to certain criminal intelligence and investigative data as more fully described below.

BACKGROUND

1) FDLE is authorized by law (Subsection 943.03(5), F.S. and Section 943.05, F.S.) to enter into agreements and become part of federal and intrastate systems for the collection and exchange of criminal history records and other information relating to crimes, criminals and criminal activity. FDLE has entered or will enter into an agreement with a coalition of other agencies for the purposes of sharing criminal justice information and intelligence. Such agencies are collectively designated as the Multistate Anti-Terrorism Information Exchange (MATRIX). By agreement, the MATRIX Executive Policy Group (hereinafter known as the Board) has designated FDLE as the Security Agent for the MATRIX Project.

2) In support of the MATRIX Project, the MATRIX coalition agencies have selected Seisint, Inc. (Seisint) as the application service provider, as reflected in that certain Contract between the Institute for Intergovernmental Research (IIR) and Seisint, whereby IIR, acting on behalf of the MATRIX coalition agencies, agreed to reimburse Seisint, from a U.S. Department of Justice grant and a U.S. Department of Homeland Security grant approved for this purpose, for the provision of Factual Data Analysis and Other Services to the MATRIX Project. FDLE has entered into an agreement with Seisint specifying the conditions under which certain data in FDLE's custody and control will be searched against certain specified proprietary databases owned by Seisint. The data resulting from this search process, involving MATRIX APPLICATIONS (as used herein, this refers to the joint information system to be used by the MATRIX coalition agencies, but is not intended to displace any trademarked or commercial term in use for any of the proprietary components of that system), are available to participating MATRIX agencies via the riss.net network, the Law Enforcement Online (LEO) network and the FDLE-provided Criminal Justice Network (CJNet). Not all MATRIX APPLICATIONS functionality will be available to all Agencies. The Board reserves the right to determine the level of access to specific data and queries each Agency will have.

3) The Board agrees to provide the Agency with such state criminal history records and information for law enforcement investigative or intelligence purposes as may be

EXHIBIT F

contained in any MATRIX APPLICATIONS system and legally available to the Agency and its operators. While the data will consist of individual records that are public as well as individual records that are exempt from disclosure under the various applicable State and Federal laws, the results of the searches referred to above constitute active criminal investigative or intelligence information.

4) The Agency is a duly authorized law enforcement agency as approved by the Board and desires the services of the MATRIX Project in order to carry out functions associated with law enforcement investigation or intelligence operations, and the Board is willing to provide such services to the Agency, provided the Agency strictly complies with this Agency Security Agreement and all applicable federal and state laws, rules and regulations.

5) FDLE has received criminal justice information systems funding from the United States Department of Justice and is subject to and must, therefore, demand that the Agencies accessing its criminal history record services through MATRIX APPLICATIONS likewise adhere to applicable federal regulations relating to the collection, handling and dissemination of state criminal history record information derived there from, as set forth in 28 C.F.R., Subpart 20B. Additionally, the Agency agrees to adhere to all applicable policies, current and future, set forth and defined by FDLE or the FBI in the Criminal Justice Information Services Security Policy.

CONDITIONS OF ACCESS AND USE

1) The Agency acknowledges information obtained from MATRIX APPLICATIONS can only be used for legitimate law enforcement investigative or intelligence purposes. A legitimate law enforcement investigative or intelligence 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 intelligence lead that requires follow-up. Law enforcement investigative or intelligence purposes do not include routine non-law enforcement background screening functions an agency may wish to conduct, whether authorized or not.

2) The Agency agrees that information retrieved from MATRIX APPLICATIONS cannot be sold, published or disclosed for commercial purposes, nor without the prior approval of the contributing agency, and is not to be made available to unauthorized persons. The Agency further agrees it is the Agency's responsibility to insure that Agency's employees' access to MATRIX APPLICATIONS is for authorized law enforcement investigative or intelligence purposes only, and to regulate such employees' proper use of the system and information at all times.

3) The Agency agrees that access to information contained within MATRIX APPLICATIONS will be granted only to law enforcement agency personnel who have been properly 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 Board. The Agency will be responsible for

completion of the Individual User Agreements for all users in their state. (See Attachment One)

4) The Agency agrees to take necessary measures to make access to MATRIX APPLICATIONS secure and prevent any unauthorized access or use. FDLE reserves the right to object to security measures, qualifications and number of personnel who will be accessing MATRIX APPLICATIONS and to suspend or withhold service until such matters are corrected to its reasonable satisfaction and that of the Board. FDLE further reserves the right to conduct inspections concerning the proper use and security of MATRIX APPLICATIONS data. Personnel of the Agency may accompany such inspections.

5) The Agency agrees to provide security for information derived from MATRIX APPLICATIONS in accordance with applicable laws, rules, and regulations and train personnel who receive, handle or have access to criminal history records or other sensitive information as to those requirements.

6) The Agency agrees to require all personnel under its control having access to MATRIX APPLICATIONS to abide by the following rules. Furthermore, the Agency understands access to MATRIX APPLICATIONS can be denied or rescinded for failure to comply with the following:

   (a) The Agency code will be used only to perform official law enforcement investigative or intelligence-related duties.

   (b) Individual passwords will not be disclosed to any other person except as authorized by Agency management.

   (c) Individual passwords will be changed if authorized personnel of the Agency suspect the password has been improperly disclosed or otherwise compromised.

   (d) The Agency agrees to perform approved background checks on Agency personnel who will have direct access to MATRIX APPLICATIONS, information, and remote access rights.

7) FDLE agrees, upon the Agency's request, to assist the Agency in its staff orientation regarding the privacy and security requirements imposed by state and federal laws, rules and regulations.

DISSEMINATION LOG

1) Dissemination of MATRIX APPLICATIONS information can only be to a law enforcement agency for law enforcement investigative or intelligence purposes. The Agency agrees to 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 data

designated by the Board, for at least five years. This record will reflect as a minimum: (1) date of release; (2) to whom the information relates; (3) to whom the information was released (including address and telephone number); (4) the State Identification (SID) and/or the FBI number(s) or other information that clearly identifies the data that were released; and (5) the purpose for which the information was requested.

2) Original source data must be used for any other dissemination.

3) The Agency agrees to retain such records for a minimum of five years and to provide FDLE access to Agency's records of dissemination.

4) The Agency agrees to allow FDLE reasonable access to its facilities and records to conduct audits to ensure compliance with this Agreement and with other applicable laws, policies and regulations.

LIABILITY

1) The Agency understands FDLE, its officers, and employees shall not be liable in any claim, demand, action, suit, or proceeding including, but not limited to, any suit in law or in equity, for damages by reason of, or arising out of, any false arrest or imprisonment or for any loss, cost, expense or damages resulting from or arising out of the acts, omissions, or detrimental reliance of the personnel of the Agency in using or relying upon information in the MATRIX APPLICATIONS information system.

2) To the maximum extent permitted by law, the Agency agrees FDLE shall not be liable for any damages whatsoever arising out of or related to the use or inability to use MATRIX APPLICATIONS, even if FDLE has been advised of the possibility of such damages. This Agreement does not constitute a waiver of any defense or immunity lawfully available to FDLE.

PROVISIONS INCORPORATED

The Agency shall be bound by applicable federal and state laws, federal regulations and the rules of FDLE to the same extent that Agency would be if such provisions were fully set out herein. Moreover, this Agreement incorporates both present and future law, regulations and rules. The Agency may terminate this Agreement as described below if the changes in law, regulations or rules are not acceptable to the Agency.

TERMINATION

Each party retains the right to discontinue service, without cause, provided written notice of forty-five days is given by U. S. mail. Each party may also terminate this agreement for cause. More particularly, FDLE reserves the right to discontinue service, without notice, upon presentation to it of reasonably credible evidence that the Agency has violated or is violating this Agreement or any pertinent federal or state law or rule.

Moreover, cause may also be deemed to exist if any term of this Agreement is found to be invalid, if any change in the laws applicable to either party requires either party to curtail performance hereunder, or if changed circumstances require either party to perform substantially more or less than was envisioned at the time this Agreement was executed. In such circumstances, the other party may terminate performance or demand renegotiation upon written notice to the other party that the changed circumstances, if known at time of execution of this Agreement, would have foreclosed that party's entry into the Agreement.

DISCLAIMER

The Agency acknowledges the law enforcement data and commercially available data sources used in the MATRIX APPLICATIONS system may contain errors, and that the Agency remains solely responsible for the interpretation, dissemination, and use of any information derived from the MATRIX APPLICATIONS system. The MATRIX APPLICATIONS system should not be relied upon as absolutely accurate, complete, or current. The Agency acknowledges that before taking action in reliance on any data in MATRIX APPLICATIONS, the Agency should independently verify that the data is accurate, complete, and current.

ACCOUNTABILITY

To the extent provided by law, the Agency agrees to be responsible for the negligent acts or omissions of its personnel arising out of or involving any information contained in or received from MATRIX APPLICATIONS.

IN WITNESS WHEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

NAME OF AGENCY: Pennsylvania State Police

HEAD: Colonel Jeffrey B. Miller **TITLE: Commissioner**
(PLEASE PRINT)

AGENCY HEAD Col. Jeffrey B. Miller
(SIGNATURE)

DATE: November 17, 2003

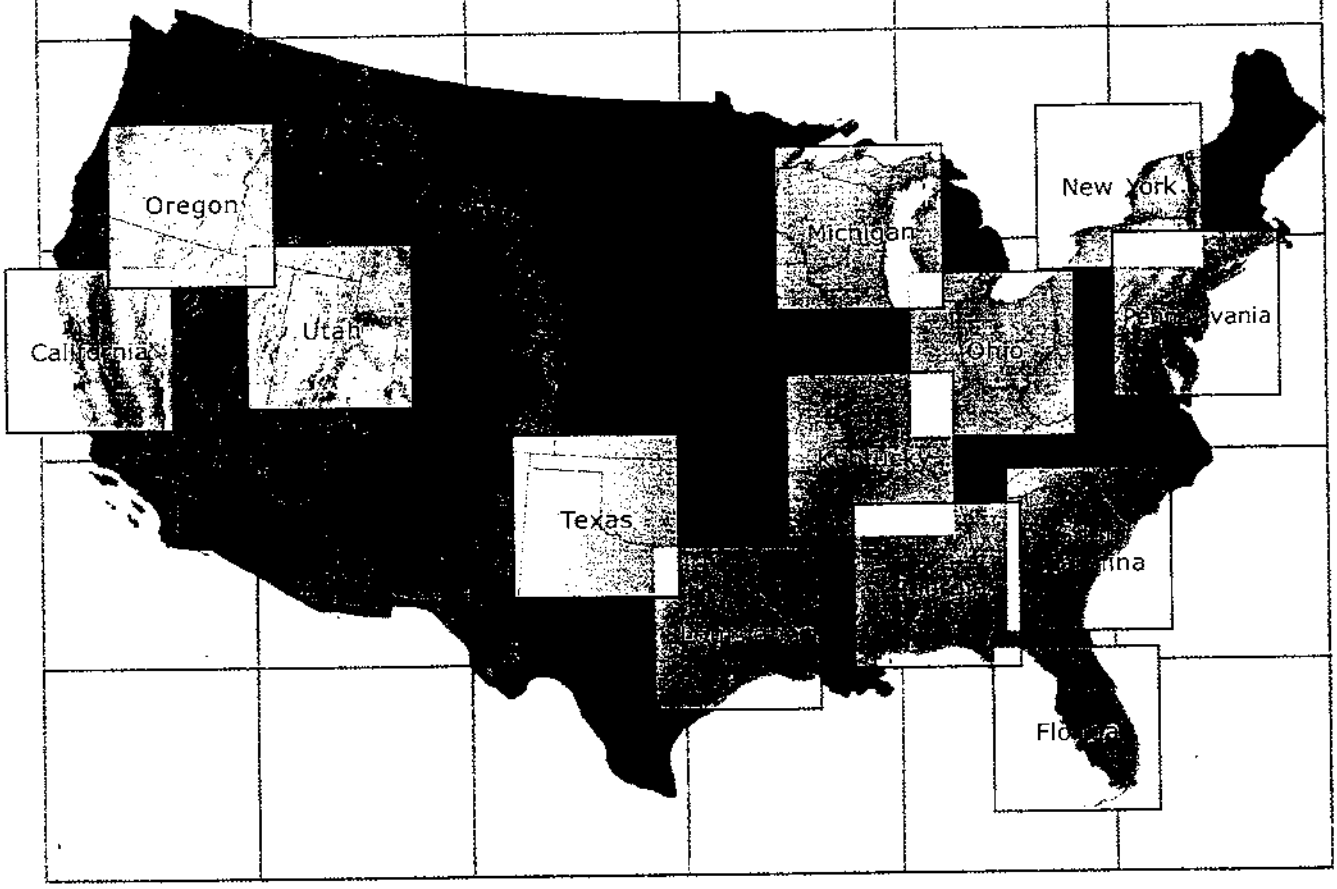
FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY _____ **TITLE** EAC

DATE 11-19-03

MATRIX

Multistate Anti-TeRrorism Information EXchange



MATRIX Project—a pilot effort to increase and enhance the exchange of sensitive terrorism and other criminal activity information between local, state, and federal law enforcement agencies

EXHIBIT
G

MATRIX—Multistate Anti-TeR

The Office of Justice Programs, U.S. Department of Justice, awarded funding for a pilot, proof-of-concept project titled the Multistate Anti-Terrorism Information Exchange (MATRIX). The MATRIX pilot project was initiated in response to the increased need for timely information sharing and exchange of terrorism-related information among members of the law enforcement community.

- The MATRIX pilot project is an effort to increase and enhance the exchange of sensitive terrorism and other criminal activity information between local, state, and federal agencies.
- The project leverages and integrates existing and proven technology to provide a new capability to assist law enforcement in identifying and analyzing terrorist and other criminal activity, and appropriately disseminating information to law enforcement agencies nationwide in a secure, efficient, and timely manner.

Organizational Structure

The organizational structure for operation of the MATRIX pilot project ensures each participant a voice in the project administration. The MATRIX pilot project has been awarded a $4 million budget by the Office of Justice Programs, Bureau of Justice Assistance, U.S. Department of Justice, for:

1. Database integration
2. Hardware
3. Software
4. Network support to a multistate coalition of law enforcement agencies

Thirteen states have been selected for inclusion in the pilot project, with the desire to expand the system nationwide once the pilot testing is completed and the success of the concept documented.

The project has three primary object

Use factual data analysis from existing data sources and data integration technology to improve the usefulness of information contained in multiple types of document storage systems

The MATRIX project is implementing factual data analysis from existing data sources to integrate disparate data from many types of Web-enabled storage systems to identify, develop, and analyze terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information within the participating states, including criminal history, driver license data, vehicle registration records, and incarceration/ corrections records including digitized photographs, with significant amounts of public data record entries. Provision has been made for the inclusion of data sources from additional states, should expansion be authorized. The use of factual data analysis from existing data sources will save countless investigative hours and significantly improve the opportunity for successful conclusion of investigations.

Data Security

Information submitted by a state may only be disseminated in accordance with any restrictions and conditions placed on it by the submitting state, pursuant to the submitting state's laws and regulations. **Information will be made available only to law enforcement agencies, and on a need-to-know and right-to-know basis.** Data access permissions will be conditioned on the privileges of the user making the inquiry.

orism Information EXchange

s:

Provide a mechanism for states to become nodes on the RISS secure intranet (riss.net) for electronic information exchange among participating agencies

The communications backbone for the MATRIX project is the Regional Information Sharing Systems (RISS) network called riss.net, which is an existing secure network with a proven track record of transmitting sensitive information among law enforcement agencies. In addition to linking the six regional RISS center resources, this network currently provides connectivity for the High Intensity Drug Trafficking Areas, United States Attorneys' Offices, other federal agencies, and several state law enforcement systems. This network is based on standards that will allow other state and federal systems to interoperate. The riss.net system represents a cost-effective solution and a way to rapidly implement the project.

Each of the 13 participating MATRIX state agencies is establishing electronic connection as a node on riss.net. End-user accounts will be enabled for authorized participating state and local law enforcement agency users in each state. This connectivity will allow secure communications with other participating agencies, as well as the RISS centers, and allow secure access to the Web-enabled document storage systems.

Encourage the exchange of information via secure state Web sites

For networking and information sharing to be effective, data must be made available over the network to authorized users. **Utilizing the access controls employed by the RISS system, secure Web sites are being created and deployed for each state** to enable information to be disseminated to the appropriate audience. These Web sites provide a familiar vehicle for MATRIX participants to post and review anti-terrorism and alert information.

This system will ensure that state and local law enforcement officers—the individuals most likely to come into direct contact with terrorists or other criminals—have the best information (accurate and complete) available to them in a timely manner. It will also provide a mechanism for local officers to share important information they collect "on the street" with other local, state, and federal authorities. **Implementation of this pilot capability represents an important component of an overall prevention strategy, critical to United States homeland security.**

The MATRIX pilot project integrates existing and proven technology to provide a new capability to assist law enforcement

For more information:

Commissioner James T. Moore
Florida Department of Law Enforcement
Chairman of the MATRIX Executive Committee
Phone: (850) 410-7001
E-mail: timmoore@fdle.state.fl.us

Mr. R. Clay Jester
Institute for Intergovernmental Research
MATRIX Project Coordinator
Phone: (850) 385-0600, extension 279
E-mail: cjester@iir.com

MATRIX pilot project participating states and the contacts in each state

California

Mr. Patrick N. Lunney
Director
California Department of Justice

Mr. George Vinson
Special Advisor on State Security
California Governor's Office

Florida

Commissioner James T. Moore
Florida Department of Law Enforcement

Georgia

Mr. Vernon Keenan
Director
Georgia Bureau of Investigation

Kentucky

Major Michael Sapp
Kentucky State Police

Louisiana

Lieutenant Colonel Mark Oxley
Louisiana State Police

Michigan

Lieutenant Colonel Robert Bertee
Michigan State Police

New York

Lieutenant Colonel Steven Cumoletti
New York State Police

Ohio

Mr. John Monce, Jr.
Superintendent
Bureau of Criminal Identification and Investigation
Ohio Office of the Attorney General

Oregon

Mr. Ronald C. Ruecker
Superintendent
Oregon State Police

Pennsylvania

Lieutenant Colonel Ralph Periandi
Pennsylvania State Police

South Carolina

Chief Robert M. Stewart
South Carolina Law Enforcement Division

Texas

Chief Marshall Caskey
Texas Department of Public Safety

Utah

Mr. Verdi White
Deputy Assistant
Utah Governor's Office

rev. 02/03

Multistate Anti-Terrorism Information Exchange (MATRIX)

Factual Analysis Criminal Threat Solution (FACTS)

Privacy Policy

Table of Contents

Section 1: Purpose 1

Section 2: Collection Limitation 2

Section 3: Data Quality 3

Section 4: Use Limitation 4

Section 5: Security Safeguards 5

Section 6: Openness 6

Section 7: Individual Participation 7

Section 8: Accountability 8

Section 1: Purpose

The Office of Justice Programs, U.S. Department of Justice, provided initial funding for a project titled the Multistate Anti-Terrorism Information Exchange (MATRIX), and additional funding was provided by the U.S. Department of Homeland Security. The MATRIX project was initiated in response to the increased need for timely information sharing and exchange of terrorism-related information among members of the law enforcement community. The project is governed by the MATRIX Executive Board which is comprised of the head or designee of each participating state agency.

Factual Data Analysis

The MATRIX project is implementing factual data analysis with a program known as the Factual Analysis Criminal Threat Solution (FACTS) by using existing nonintelligence data sources to integrate disparate data from many types of storage systems to identify, develop, and analyze information related to terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information between the participating states, including criminal history, driver license data, vehicle registration records, and incarceration/corrections records with significant amounts of public data record entries. None of the data sources accessed are recognized as intelligence databases as defined by the criminal intelligence systems operating policies contained in 28 CFR Part 23. The use of factual data analysis from existing data nonintelligence sources will save countless investigative hours and significantly improve the opportunity for successful conclusion of investigations.

Section 2:
Collection Limitation

The FACTS application is maintained for the purpose of sharing information by agencies participating in the MATRIX project. The FACTS application contains copies of the original source data provided by the states participating in the MATRIX project, periodically refreshed, in an efficient and automated environment. The decision of the states to participate in MATRIX and about which databases to provide is voluntary and will be governed by the laws of the individual state respecting such data, as well as by applicable federal law such as the Driver's Privacy Protection Act of 1994.

Because the laws, rules, or policies governing information that can be collected and released on private individuals will vary from state to state, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information is to abide by the collection limitations applicable to it by reason of law, rule, or policy. Information contributed to the FACTS application should be that which has been collected in conformance with those limitations.

Section 3:
Data Quality

The states participating in the MATRIX project remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the FACTS application.

Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the FACTS application. In order to maintain the integrity of the MATRIX project, any information obtained through the FACTS application must be independently verified with the original source from which the data was extrapolated *before* any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

Section 4:
Use Limitation

Information obtained from or through the FACTS application can only be used for legitimate law enforcement investigative purposes. A legitimate 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.

The Florida Department of Law Enforcement (FDLE), acting as the Security Agent for the MATRIX project, will take necessary measures to make certain that access to the FACTS application is secure and will prevent any unauthorized access or use. FDLE reserves the right to restrict the qualifications and number of personnel who will be accessing the FACTS application and to suspend or withhold service to any individual violating this *Privacy Policy*. FDLE, or persons acting on behalf of the MATRIX Board, further reserves the right to conduct inspections concerning the proper use and security of the FACTS application's data.

Security for information derived from the FACTS application will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to criminal history records or other sensitive information will be trained as to those requirements.

All personnel having access to the FACTS application agree to abide by the following rules:

(a) The FACTS application will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.

(b) Individual passwords will not be disclosed to any other person except as authorized by agency management.

(c) Individual passwords will be changed if authorized personnel of the agency or FDLE suspect the password has been improperly disclosed or otherwise compromised.

(d) Background checks will be completed on personnel who will have direct access to the FACTS application.

(e) Use of the FACTS application in an unauthorized or illegal manner will subject the user to denial of further use of FACTS, discipline by the user's employing agency, and/or criminal prosecution.

Each authorized user understands that access to the FACTS application can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

Section 5:
Security Safeguards

Information obtained from or through the FACTS application will not be used or publicly disclosed for purposes other than those specified in the Agency Security Agreement that each participating agency must sign. Information cannot 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.

Use of the FACTS application is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the FACTS application will be granted only to 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 MATRIX Board of Directors. Each individual user must complete an Individual User Agreement in conjunction with training provided by a certified FACTS Trainer.

Access to the FACTS application will only be allowed over the Regional Information Sharing Systems (RISS) secure network, commonly known as riss.net, the FBI's secure Law Enforcement Online (LEO) network, and the state of Florida's secure Criminal Justice Network.

Section 6: Openness

It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data (e.g., a participating state's motor vehicle department) as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

All agencies participating in the MATRIX project will make this *Privacy Policy* available for public review or to any interested party. The MATRIX project will post this *Privacy Policy* on its public Web site and make it available to any interested party.

Section 7:
Individual Participation

The data maintained in the FACTS application is provided, on a voluntary basis, by the participating MATRIX states or is information obtained from other sources by Seisint, Inc. The data is made available "as-is" and is not to be viewed as necessarily accurate, complete, or current until verified with the original source. The process of using each contributor's data against the information contained in the FACTS databases will involve comprehensively comparing and cross-referencing the former for any matches, similarities, or points of commonality with the latter, without limitation or restriction as to the kind or quantity of information thereby derived or produced.

Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination, and use of any information which results from the search process 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 cannot access individually identifiable information, on themselves or others, from the FACTS application. 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 participating state 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 query is made to the FACTS application, the original request is automatically logged by the system identifying the user initiating the query. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement investigative purpose. The agency *from* which the 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 data designated by the Board, for at least five years. This 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 must be used for any official action. 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. FDLE, as the Security Agent for MATRIX, will be responsible for conducting or coordinating audits and investigating misuse of the FACTS application. The MATRIX Privacy Committee, appointed by the Chair of the Executive Board, may also conduct audits on behalf of the Board. All violations and/or exceptions shall be reported to the MATRIX Board.

Individual users of the FACTS application remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use limitations for the use of the FACTS application may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the MATRIX project is required to abide by this *Privacy Policy* in the use of information obtained by and through the FACTS application.