Multistate Anti-Terrorism Information Exchange (MATRIX)

Frequently Asked Questions

What Is MATRIX?

The Multistate Anti-Terrorism Information Exchange (MATRIX) is a pilot, proof-of-concept project initiated in response to the increased need for timely information sharing and exchange of terrorism-related and other criminal information among members of the law enforcement community. The MATRIX project is a tool that will help ensure that local and state law enforcement officers have timely, accurate, and effective information.

In January 2002, a group of state law enforcement executives from throughout the United States met to discuss domestic security problems and challenges, and to develop proposed solutions to increase sharing throughout all levels of law enforcement. A multistate coalition of state law enforcement agencies resulted from this meeting.

What is FACTS?

One of the MATRIX applications, known as the FACTS system, provides law enforcement a technological, investigative tool allowing query-based searches of billions of available state and public records. FACTS is short for Factual Analysis Criminal Threat Solution. Using FACTS, an investigator can conduct a query using incomplete information, such as a portion of a vehicle license number. FACTS will search the system and assemble information matching the partial description.

Why is MATRIX important?

It is critical for law enforcement agencies to respond quickly to criminal activities. They must capitalize on twenty-first century tools to combat twenty-first century threats. Prior to MATRIX, investigators would compile investigative information manually via multiple independent databases, making numerous phone calls or visiting county records offices. The MATRIX project, through the FACTS application, makes this same information available in seconds.

How is MATRIX funded?

The Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. awarded $4 million to the MATRIX project, which has paid for connectivity for participating agencies to the network known as riss.net, secure Web site development within the participating states, 34 user licenses to the FACTS application per participating state, and some initial assimilation of data. An additional $8 million has been received from the Office for Domestic Preparedness, U.S. Department of Homeland Security, to expand system access for one year, along with a significant increase in the number of user licenses available to the agencies. A long-term funding strategy is under development.

Who controls MATRIX?

The MATRIX Board of Directors, comprised of law enforcement executives from the participating states, represents the interests of the MATRIX participants in a project oversight capacity. The Board oversees implementation and operation of the project, including funding, expenditures, and operational policies and procedures governing the sharing of information among local, state, and federal law enforcement agencies, as well as coordinating those activities with the Regional Information Sharing Systems (RISS).

What is the relationship between MATRIX and RISS?

The communications backbone for the MATRIX project is the RISS secure intranet called riss.net. Each of the participating MATRIX state law enforcement agencies may establish an electronic connection as a node on riss.net. End-user accounts will be enabled for authorized participating local, state, and federal law enforcement agency users in each state.

Is MATRIX an intelligence system?

No. MATRIX is not an intelligence system. It is an information sharing initiative of the participating states, which allows investigators to share information and query billions of available state and public records in seconds. MATRIX does not provide access to magazine subscription lists, reading lists, telephone calling records, bank transactions, lists of credit cards, or credit card transactions. Under federal law, when such data is required in law enforcement investigations, it can only be obtained with a judicial order.

Are any intelligence systems linked to the FACTS application?

No. Only databases that have been contributed for inclusion by participating states or containing information provided by Seisint, Inc. are included in FACTS. This information has

been accessible by law enforcement for many years. The only difference is that FACTS allows for the review of billions of state and public records simultaneously. Previously, retrieving the data required investigators to manually "pull" records, query multiple database systems, and make a number of phone calls to obtain the same information FACTS provides.

WILL MATRIX BEGIN COLLECTING INTELLIGENCE DATA ON INDIVIDUALS?

No. There is no new collection effort involved with compiling and combining information for MATRIX participants nor are there any intentions to create an intelligence database via the MATRIX initiative. The sole purpose of MATRIX is to provide already existing information to law enforcement investigators in a timely and accurate manner.

DOES MATRIX STORE DOSSIERS ON INDIVIDUALS?

No. Reports are generated based on specific investigative queries of the systems by investigators. Leads are generated for investigator verification and follow-up.

IS MATRIX SUBJECT TO 28 Code of Federal Regulations (CFR) Part 23?

No. MATRIX does not operate any criminal intelligence databases. Intelligence may be accessed via the network known as riss.net. However, the individual owner of the intelligence system would be responsible for compliance with 28 CFR Part 23.

IS MATRIX DIFFERENT THAN TERRORISM INFORMATION AWARENESS (TIA)? IF SO, HOW?

Yes. The MATRIX FACTS application is different than the Terrorism Information Awareness (TIA) system. The purpose of TIA, formerly known as Total Information Awareness, was to track information on people so that the Department of Defense could detect potential terrorists and criminals. TIA sought to collect as much information about people as possible. TIA also had a number of technological components to help the government identify and track individuals, identify patterns of behavior, and correlate relationships and associations. The MATRIX project provides data to an investigator based on a query; information obtained as a result of the query is then analyzed. The results of the query and analysis would be considered active criminal intelligence.

WHAT TYPES OF INFORMATION IS STORED IN FACTS AND WHERE DOES IT COME FROM?

FACTS contains information from criminal history, driver's license, vehicle registration and incarceration/corrections (including digitized photographs) databases, as well as significant amounts of public and commercial data.

Accurint provides public and commercial records obtained through the MATRIX FACTS program. Accurint is an information management and technology company. Accurint stores billions of records that can be searched, analyzed, and compiled quickly. Accurint assists a number of businesses and industries including law enforcement. Some of the types of data available through Accurint include bankruptcies, concealed weapons permits, directory assistance, FAA aircraft and pilots, federal firearms and explosives licenses, Internet domain names, professional licenses, and voter registrations. There are no magazine subscriptions, purchasing habits, employment or income history. For more information regarding Accurint, visit their Web site at http://www.accurint.com.

The FACTS application contains copies of the original source data provided by participating states, periodically refreshed, in an efficient and automated environment. The decision of states to participate in MATRIX, as well as which information sources to provide, is voluntary and are governed by the laws of the individual state providing such data, as well as applicable federal law, such as the Driver's Privacy Protection Act of 1994.

The information available through the MATRIX project has been accessible to law enforcement for many years. Much of the information is available to the general public. Some of the same information is available on the Internet through sources such as US Search, Intelius, and NetDetective. Some states have public record laws that provide criminal history records to the public. It is information from existing sources that is now being combined and made accessible to law enforcement personnel in a manner that allows them to react quickly to threats.

HOW IS THE ACCURACY OF THE INFORMATION AVAILABLE THROUGH FACTS VERIFIED?

The participating states are the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data. 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 information obtained through FACTS, any information 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.

HOW DO STATE LAWS IMPACT RECORD DISSEMINATION FOR FACTS?

The laws governing access to public record information in each state address what data is made available from those record sources. The FACTS system is structured to be in compliance with the laws of each participating state and by policy; the Board of Directors agreed that the MATRIX capability could be used only in the pursuit of a criminal investigative matter.

WILL FACTS TAKE THE PLACE OF THE INVESTIGATIVE PROCESS?

No. FACTS provides an improved "tool" for law enforcement investigators, not a substitute for the investigation itself. It is investigator-driven, not automatic. FACTS simply provides access to information in a centralized fashion that is already available to the investigator. Each investigator will continue to develop his or her investigative basis for a search or other enforcement action and is required to independently verify data before relying upon it for arrests, searches, or other significant enforcement action. A search is not that different from what Internet users do when they type in a query on an Internet search engine. That search engine compiles responses from numerous sources and makes them available for review. Likewise, the FACTS application compiles responses from numerous sources and makes them available to the investigator.

In addition, FACTS can associate the responses to suggest factors that may confirm investigative efforts or help identify potential ongoing criminal conspiracies or developing criminal activity. The MATRIX project puts available state records and public or commercially available information in one place where it can be accessed quickly and simultaneously, rather than at each source, one source at a time. It helps focus investigative efforts. In short, it helps equip law enforcement investigators with the information needed to detect and respond to criminal and terrorist threats.

DOES MATRIX MONITOR ALL CITIZENS?

No. The FACTS system does not allow indiscriminate surveillance of one's activities, and it does not "monitor" individuals. Inquiries will be driven by actual criminal investigations or domestic security threat information, and the use of applications available through the MATRIX project will be monitored to guard against inappropriate or unauthorized use.

DOES MATRIX CONSIDER PRIVACY RIGHTS? IF SO, HOW?

Yes. Maintaining privacy is paramount to MATRIX. The U.S. Department of Justice (DOJ) remains committed to ensuring that individual's privacy rights are observed. In situations where there is a legitimate law enforcement or public safety purpose to initiate law enforcement investigations, law enforcement agencies are expected to follow long-standing agency and judicial procedures that govern these situations.

A privacy policy has been developed which provides the rules related to collective limitations, use limitations, data quality, openness, and accountability. This policy must be adhered to by participating agencies. Users of MATRIX will receive training and will be subject to a background investigation. In addition, a Privacy Committee has been established to monitor use.

The system also helps protect innocent persons and helps prevent enforcement actions taken on the basis of incomplete or out-of-date information. In this regard, the MATRIX project helps protect persons against unwarranted police intervention. DOJ supports several initiatives dealing with this topic and has received input from various organizations on model privacy guidelines and practices, such as the Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group. Additional information regarding Global can be found at www.it.ojp.gov/global.

WHAT SECURITY MEASURES ARE IN PLACE TO ENSURE PROPER USE OF MATRIX?

Use of applications available through the MATRIX project is guided by the premise that law enforcement agencies should not access, analyze, or use personal information on individuals without a nexus to suspected terrorist or other illegal activity. 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 MATRIX applications is secure to prevent any unauthorized access or use. FDLE reserves the right to restrict the qualifications and number of personnel who will be accessing the applications and to suspend or withhold service to any individual violating this policy.

FDLE reserves the right to conduct inspections concerning the proper use and security of MATRIX application data by MATRIX users and their agency. An audit log is maintained by the application for automated system dissemination. Each agency must maintain a log of "secondary" disseminations to authorized agency staff. In addition, FDLE implemented user agreements for licensees and member agencies that set forth the standards, policies, procedures, and guidelines that govern access.

Before officers are allowed to access information through MATRIX, they must pass background screening investigations within their agencies, obtain approval from their agency head, and receive appropriate training and the necessary security protocols that allow them to achieve access. Use of any MATRIX application in an unauthorized or illegal manner will subject the user to denial of further use of the application, discipline by the user's employing agency, and/or criminal prosecution.

HOW DOES MATRIX USE FACTUAL DATA ANALYSIS?

The MATRIX project is implementing factual data analysis with 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's license data, vehicle registration records, and incarceration/corrections records with significant amounts of public data-record entries.

CAN THE PUBLIC REVIEW MATRIX DATA CONCERNING THEMSELVES?

No. Members of the public cannot access individually-identifiable information on themselves or others. 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 Code of Federal Regulations, Section 20.21(g).

WHO IS THE INSTITUTE FOR INTERGOVERNMENTAL RESEARCH (IIR)?

The Institute for Intergovernmental Research (IIR) is a Florida-based nonprofit research and training organization specializing in law enforcement, juvenile justice, and criminal justice issues.

WHAT IS THE ROLE OF IIR?

IIR serves as the Bureau of Justice Assistance and U.S. Department of Homeland Security grantee for MATRIX and is responsible for all financial matters regarding the project and administrative support, such as meeting coordination and preparation of written documents.

WHO IS SEISINT, INC.?

Seisint, Inc. is a global information management and technology company providing products that allow organizations to quickly and easily extract valuable knowledge from large amounts of data. Seisint's products are made possible by integrating Seisint's Data Supercomputer technology, multitudes of available state and public records, and patent-pending data-linking methods. Seisint was founded in 1998 and has grown to employ over 200 people at its locations in Boca Raton, Florida; Orlando, Florida; and London, England.

Seisint Senior Management

Mr. Paul S. Cameron – President & Chief Executive Officer
Ms. Christiane Breton – Chief Financial Officer
Mr. Armando Escalante – Chief Operating Officer
Mr. Kenneth J. Schwartz – General Counsel
Mr. James P. Swift – Executive Vice President

Seisint Board of Directors

Mr. Jack Hight – Chairman
Ms. Martha Barnett
Mr. Bruce Barrington
Mr. Leon Brauser
Mr. Joel Friedman
Mr. Paul S. Cameron
Mr. Ira Siegel

For more information regarding Seisint's senior management and Board of Directors, visit www.seisint.com.

WHAT IS ACCURINT?

Accurint is a Seisint product housing billions of records on individuals and companies. Law enforcement can use Accurint for searching information on people, their associations, locations, etc. For more detailed information, visit www.accurint.com. The information contained in Accurint was available prior to FACTS. FACTS leverages this resource.

HOW IS THE FEDERAL GOVERNMENT ABLE TO PROVIDE A PRIVATE COMPANY WITH PUBLIC FUNDS TO ADMINISTER THE MATRIX PROJECT?

The MATRIX project is a law enforcement criminal interdiction initiative. No private company administers MATRIX. The MATRIX Board of Directors provides policy oversight and guidance. FDLE administers site operations. The federal government can enter into grants and cooperative agreements with local, state, and tribal units of government, educational institutions, and private nonprofit organizations. In select instances, with proper justification and prior approval from the grant-issuing agency, grant recipients can obtain "sole source" approval to work with private vendors. The grantee submitted a request to the Bureau of Justice Assistance (BJA) along with a justification, seeking approval to use a private company's (Seisint) computer software and information technology engineering product on a "sole-source" basis. Seisint had previously developed analytical tools for commercial business applications that automated many of the processes used to categorize information from public sources. It was these tools that provided the basis for the FACTS tool on which MATRIX was developed.

IS THE SEISINT FACILITY AND DATA WAREHOUSE SECURE TO MAINTAIN FACTS DATA?

Yes. In August 2003, FDLE members conducted an audit of the Seisint facility and application resources. The audit team found that an appropriate level of physical security is present at the Seisint facility to secure FACTS. The facility is secured via biometrics technology. One FDLE member is assigned to the MATRIX project as the Information Security Officer. The audit team also found that Seisint is using the latest available technology to protect the FACTS data. Appropriate policies are also in place to maintain and protect the confidentiality and integrity of the data.

WHAT IS THE STATUS OF SEISINT EMPLOYEE BACKGROUND INVESTIGATIONS?

The FDLE Miami Regional Operations Center and Office of Statewide Intelligence conducted a detailed background investigation on Seisint Chief Executive Officer Paul Cameron, Seisint founder Hank Asher, and all Seisint employees with access to data. The background investigations included a review of criminal, financial, corporate, credit, and

other public records, including a fingerprint check, as well as a review of FDLE and other law enforcement agency investigative and intelligence files.

In regard to Mr. Cameron, his background investigation indicated no previous criminal history and no inappropriate financial or business records. In addition, no significant irregularities were discovered in any of the backgrounds conducted on Seisint personnel with direct access or contact with information.

FDLE's investigation of Mr. Asher revealed some involvement with drug smuggling. Based on interviews with law enforcement personnel, individuals who had been involved in smuggling, and Mr. Asher's own statements, it was confirmed he had been involved in smuggling in the early 1980s, although he was never arrested or charged. Other issues were investigated and noted appropriately in the final report. As a result of the investigation, Mr. Asher resigned from Seisint's Board of Directors on August 29, 2003. In addition to severing his official relationship with the organization, Mr. Asher has placed his stock shares into a voting trust to be managed by individuals outside the corporation. He has no access to data provided by the FACTS application by any of the state agencies.

WHAT ENTITIES ARE ABLE TO PARTICIPATE IN MATRIX AND HOW DO THEY JOIN THE INITATIVE?

Currently, only primary state law enforcement agencies are involved with the MATRIX project. However, the Board of Directors is in the process of establishing guidelines for other entities, such as local and federal law enforcement agencies, to participate in the project.

HOW DO STATES BECOME INVOLVED WITH THE MATRIX PROJECT?

States interested in participating in this project may contact any MATRIX Executive Board member. The Florida Department of Law Enforcement serves as the project's security agent and may be contacted as follows:

Florida Department of Law Enforcement
Office of Statewide Intelligence
(850) 410-7060