

STATEMENT

OF

MARK A. ZADRA

Chief of Investigations  
Office of Statewide Intelligence  
Florida Department of Law Enforcement

REGARDING A HEARING ON

**Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and  
Homeland Security for Federal, State and Local Law Governments**

BEFORE THE

CONGRESS OF THE UNITED STATES  
HOUSE OF REPRESENTATIVES

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL  
RELATIONS AND THE CENSUS

July 13, 2004

2:00 PM

Room 2154 Rayburn House Office Building

Good afternoon, Chairman Putnam and distinguished Members of the Subcommittee. My name is Mark Zadra, and I am a 26-year member of the Florida Department of Law Enforcement (FDLE). I serve in a leadership capacity as Chief of Investigations within the Office of Statewide Intelligence.

FDLE is a statewide law enforcement agency that offers a wide range of investigative, technical and informational services to criminal justice agencies through its seven Regional Operations Centers, fifteen Field Offices, and seven Crime Laboratories. Its primary mission is to promote public safety and strengthen domestic security by providing services in partnership with local, state, and federal criminal justice agencies to prevent, investigate, and solve crimes while protecting Florida's citizens and visitors. FDLE utilizes an investigative strategy that comprises five primary focus areas including Domestic Security, Violent Crime, Major Drugs, Economic Crimes and Public Integrity. FDLE's Criminal Justice Information Program provides criminal identification screening services to criminal justice agencies, non-criminal justice agencies, and private citizens to identify persons with criminal warrants, arrests, and convictions. FDLE further meets the information needs of Florida's criminal justice community by providing network services including computer hardware, software programming, telecommunication costs and computer technology necessary to maintain and share information.

The Office of Statewide Intelligence's mission is to provide FDLE and other Florida law enforcement leadership with the sufficient amount and types of information to make informed decisions regarding the deployment of their investigative resources. This is accomplished primarily by conducting and disseminating crime assessments. OSI is also instrumental in the development and maintenance of investigative automation both for FDLE and the Florida criminal justice community. In support of these roles OSI operates the Florida Computer Crime Center, the Counter Terrorism Intelligence Center, the Financial Crimes Analysis Center and the Dissemination and Special Projects Unit.

## **The Multistate Anti-Terrorism Information Exchange (MATRIX) and the Florida Criminal Justice Network (CJNet)**

FDLE has for many years been a major leader and facilitator of information and intelligence sharing primarily within the State of Florida. In the wake of September 11, 2001 however, this role took on more of a national perspective as it was quickly evident that information sharing could no longer be considered effective on merely a local or regional basis. Following the horrific events of that day, a group of state law enforcement executives from throughout the United States began meeting to discuss domestic security problems and challenges, and to develop proposed solutions to increase information and intelligence sharing throughout all levels of law enforcement. With FDLE helping to lead the effort a multistate coalition of state law enforcement agencies emerged. The successes achieved and the information sharing lessons learned became the genesis for the idea behind the Multistate Anti-Terrorism Information Exchange (MATRIX) pilot project.

MATRIX is a pilot, proof-of-concept project initiated in response to the increased need for timely information sharing and exchange of terrorism and other related criminal information among members of the law enforcement community. The MATRIX project is a means that will help ensure that local and state law enforcement officers have timely, accurate, and effective information. The MATRIX project has three primary objectives:

1. Establish connectivity utilizing the existing Regional Information Sharing System (RISS) Network.
2. Secure web-based access to intelligence data and information sources contained in the participating states' intelligence systems with the objective to connect to federal systems where permitted.
3. Use data analysis and integration technology to improve the usefulness of the data contained in multiple types of record storage systems.

MATRIX is consistent with the policies and implementation guidelines detailed within the adopted National Criminal Intelligence Sharing Plan. This plan, developed at the urging of the International Association of Chiefs of Police's (IACP) by the Department of Justice's Global Justice Information Sharing Initiative, outlines specific "action steps" that can be taken immediately by almost any agency and what can be expected by performing those steps. The plan provides an in-depth discussion of the issues that hinder intelligence sharing and should serve as a guideline for any information sharing initiative.

The first objective of the MATRIX Project, connectivity, has been met through the utilization of an existing secure law enforcement communication backbone, the Regional Information Sharing System's (RISS) secure intranet known as RISSNet. This system is used by several law enforcement systems to facilitate information sharing within a secure environment.

The second objective, to provide secure web-based access to intelligence data and information sources, continues to evolve. For instance, in Florida, the Office of Statewide Intelligence maintains a secure intelligence website which previously was made available only to law enforcement within our state via Florida's secured Criminal Justice Network (CJNet). Now this secure website is available to other MATRIX participants over RISSNet. The Office of Statewide Intelligence also maintains the state's legislatively mandated Domestic Security and Counter Terrorism Database, known as ThreatNet, whereby local, state, and federal law enforcement agencies within Florida can report suspected terrorism activity and provide domestic security related intelligence. ThreatNet is accessed by all authorized participants via the CJNet.

Within Florida, CJNet serves as the infrastructure for statewide criminal justice information systems by providing secured connectivity that is limited to criminal justice agencies. This closed network or "intranet" connects approximately 700 Florida criminal justice sites at the local, state, and federal levels.

In addition to connectivity, CJNet provides electronic mail, transfer of data files and photographs, and access to various databases that are crucial or useful to the criminal justice community. Because of Florida's MATRIX participation and connectivity to RISS, the capability to access Florida's numerous CJNet applications and intelligence databases is now available to other participating states.

The third objective, factual data analysis, is being met through a very innovative and effective computer application. This application, known as the Factual Analysis Criminal Threat Solution (FACTS), provides law enforcement a technological investigative tool that allows query-based searches of state maintained and commercially available public records that are legally available to law enforcement.

State maintained and commercially available public databases have long been a source of valuable information to law enforcement investigations. The ability through FACTS to integrate state data sources such as driver license records, digital images, criminal history information, corrections data and sexual offender data, in conjunction with commercially available public data such as published telephone subscriber and property ownership records has exponentially increased its investigative value. This information can be used to help locate subjects of a criminal investigation saving countless investigative hours and significantly improving the opportunity for a successful investigative resolution. FACTS allows law enforcement officers and intelligence analysts to utilize their time more effectively and efficiently by concentrating on leads that have a greater potential for investigative relevancy. They can utilize known investigative information, however limited, and develop potential leads in seconds, versus traditional and manually intensive efforts which can take days, weeks, or months. Timeliness is crucial in life or death situations, especially when law enforcement is addressing investigations involving weapons of mass destruction, violent crime or abduction.

It is important to note that FACTS only contains information already available to law enforcement from commercially available public records and state-owned data. The application simply provides a single

point of access to information, not unlike what Internet users do when they type in a query on an Internet search engine. The FACTS database contains information which, upon query, is dynamically combined from selected commercially available public information and information provided from participating states which resides on servers secured and controlled by FDLE (serving as the State Security Agent on behalf of the MATRIX Board). There are no intelligence records contained within the FACTS application.

Authorized law enforcement users are able to perform searches of the following data sets and obtain related information such as names, addresses, dates and numbers which all are, under applicable state or federal law, available to law enforcement without subpoena or court order.

- Person
- Driver License
- Motor Vehicle/Vessel
- Telephone Directory Assistance
- Company
- Criminal History
- Department of Corrections
- Sexual Offender
- Uniform Commercial Code
- Property Deed
- Property Assessment
- Civil Court including Bankruptcy
- Government Published Watch Lists
- Professional License
- Federal Aviation Administration Certifications and Aircraft ownership

**FACTS does NOT contain:**

- Telemarketing calling lists
- Direct mail mailing lists
- Airline reservations or travel records
- Frequent flyer/hotel stay program membership or activity
- Magazine subscriptions lists or reading lists
- Telephone calling logs or records
- Credit card or debit numbers or credit history information
- Purchases (e.g., retail store, Internet, or even gas stations)
- Mortgage or car payments
- Bank account numbers or account balances
- The costs of a home addition
- Birth certificates
- Marriage licenses
- Divorce decrees
- Utility bill payments (i.e., gas, electric, phone, heating oil, cable or satellite TV)
- Medical Records
- Fingerprints

The MATRIX Board, comprised of a law enforcement policy maker from each participating state, sets all policy for MATRIX participation and the use of the FACTS application. Security agreements between the states govern who can access the system and security of the information once it is retrieved from the system. By policy, access is granted only to law enforcement agency personnel who have been approved through their employing agency and properly screened with a state and national fingerprint-based

background check. Each participating agency and individual user must complete an agreement and then be properly trained in system use including security and privacy considerations.

As also established by policy, any MATRIX computer application, including FACTS, 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 or to prevent a criminal act. The information obtained from any MATRIX application cannot be sold, published, or disclosed for commercial purposes. The FACTS application has no ability to monitor, track or surveil anyone. It is not similar to the Terrorist Information Awareness (a defunct federal program), nor is it a "data mining" program that sifts through information and then automatically suggests possible criminal activity or matches individuals to "profiles." The database is investigator-driven. Queries must be made by investigators or analysts to prompt responses. They utilize a "submit" button and not a "solve" button. Time honored investigative "shoe leather" and savvy are not replaced, but augmented. FACTS simply provides access to information in a centralized fashion that is already available to investigators at individual sites today. Each investigator still has to develop his or her investigative basis for a search or other enforcement action and is to independently verify data before relying upon it for arrests, searches or other significant enforcement action.

There are numerous protections and safeguards in place to ensure that the MATRIX system or its associated applications such as FACTS are not misused.

These include:

- Agency and user agreements that define system use
- The requirement for fingerprint based background checks on all users approved by participating agencies
- Project oversight and policy guidance (including a Privacy Policy) by the MATRIX Board
- Connectivity through a secured Regional Information Sharing System Network
- Use of encrypted tokens, user names and passwords for all users
- Sign on requirements that require the user to acknowledge use is for law enforcement purposes only and is in compliance with all established security and privacy considerations
- The requirement that users must verify data with originator prior to any official law enforcement action
- System Firewalls at numerous points of the secure network
- Logging of all user activity
- Maintenance of a system audit log for automated system dissemination. Each agency must maintain a secondary audit log of “secondary” disseminations to authorized agency staff
- Random and periodic audits of system use to identify potential misuse (misuse results in denial of further use of FACTS, discipline by the user's employing agency, and/or criminal prosecution)

FDLE at the request of the MATRIX Board serves as the MATRIX State Security Agent with members co-located on-site at the vendor's facility. MATRIX data is maintained on separate servers in an FDLE-controlled server room which is separately and securely isolated from the rest of the facility. FDLE has conducted a physical security audit/assessment of the housing facility including computer system and networking integrity. FDLE has also conducted backgrounds investigations on all vendor employees directly involved in MATRIX project

The Florida Legislature closely reviewed the MATRIX project and the FACTS application prior to authorizing Florida's participation. During March 2003, members of the Senate Homeland Defense,

Public Security, and Ports Committee and the House Coordinating Committee on Public Security viewed this system firsthand at FDLE and were confident in the system's intent, purposes, and internal limitations to prevent abuse. It is believed that these efforts during the project's initiation phase contributed significantly to a better understanding of the project, and eliminated confusion and any misperceptions about the project.

The MATRIX project has helped law enforcement officers in Florida and the other participating states to quickly and more easily obtain the information needed to investigate terrorist threats and other criminal activity. While the FACTS tool was initially developed in response to counter-terrorism investigations, it quickly became established as a tool to significantly impact investigations of all types of criminal activity. There are numerous success stories associated with FACTS use. FACTS has assisted in solving homicides, cracking "cold cases," busting fraud rings, identifying drivers of vehicles involved in hit and run, and pinpointing participants in drug investigations. FACTS has been used in identifying and locating subjects involved in investigations and even witnesses for the prosecution phase of cases. It has further been used to identify associates of case targets and vehicles involved in criminal activity. Many consider FACTS to be a success each and every time it is utilized when considering due to nothing other than the amount of time saved by investigators and analysts pursuing investigative leads.

Having timely access to complete information not only assists investigators in taking enforcement actions against suspects, it also helps protect innocent persons and helps prevent enforcement actions taken on the basis of incomplete or out-of-date information. In this regard, FACTS helps protect persons against unwarranted police intervention.

There are many misconceptions surrounding the MATRIX program that have been publicized through various sources. The following comments are offered to help clear up any inaccuracies that have emerged regarding the project, particularly with respect to the FACTS application.

- MATRIX is controlled by the participating states and not a vendor.
- The vendor is not permitted to access law enforcement data provided by the states to the Florida Department of Law Enforcement (FDLE) other than in its supporting role to MATRIX.
- FACTS is not a substitute for the now defunct Total/Terrorism Information Awareness (TIA) Project and there is no relationship to that system. Instead, it is a query/response based information source for use by trained and screened civilian law enforcement as a part of an active criminal investigation.
- The MATRIX FACTS application is not an intelligence database nor does it contain intelligence information.
- The MATRIX FACTS application only contains information already accessible to law enforcement from commercially available public records and state-owned data.
- The MATRIX FACTS application does not track or monitor individuals.
- The MATRIX FACTS application does not contain magazine subscription lists, reading lists, telephone calling records, bank transactions, lists of credit cards or credit card transactions, and; therefore, such data is not provided by MATRIX to law enforcement. Under federal law, when such data is required in law enforcement investigations, it can only be obtained under a judicial order; i.e., subpoena.
- The MATRIX FACTS application does not perform “data mining” to produce unprompted information based on established profiles

In summary, MATRIX is a project that helps assure that state and local law enforcement officers—those most likely to come into contact with criminals or terrorists in our communities—will have timely, accurate and effective information. We must have the capacity to respond quickly to developing events to combat terror. As criminal enterprises are making use of computers and technology to assist their criminal activities law enforcement must avail itself of 21<sup>st</sup> century tools to combat 21<sup>st</sup> century threats. The MATRIX project expansion is paramount to equip law enforcement analysts and investigators with

information and intelligence exchange capabilities consistent with the technology advancements integrated and woven into the fabric of our modern day society.

### **Florida's Data Integration Efforts**

Many have identified the lack of information sharing as a contributing factor to our country's inability to prevent some of the terrorist attacks in America, most notably those that occurred on September 11, 2001. In response, numerous new information sharing systems and projects continue to emerge at the national, state, and local levels. These systems can generally be categorized as systems for communication (situational awareness), criminal intelligence gathering, data retrieval, and geographical and spatial data analysis. Florida is no exception as there are at least six (6) major "data fusion or data integration" projects in various stages of development and implementation, including the MATRIX Project.

While each of these information and/or intelligence exchange efforts are laudable, it is paramount that these projects do not become individual "information silos" incapable of integrating with or being interoperable with one another. For that reason, Florida created a Data Integration Committee comprised of members of the various projects and inclusive of all seven of its regions. This committee is in the process of developing a statewide strategy for intelligence and information sharing. Among the issues being considered within the strategy are the following:

- Oversight
- Funding
- Content of Data Sharing
- Participants
- System Architecture
- Integration and Sharing with Federal Agencies
- Security

- Data Standards
- Audits
- Risk Mitigation Strategy/Misuse Consequence
- Agency and User Agreements
- Privacy Policy

### **The National Criminal Intelligence Sharing Plan**

The National Criminal Intelligence Sharing Plan outlines how collaboration could be achieved on a national level. Recommendation 2 of the Plan calls for the creation of a Criminal Intelligence Coordinating Council to advise Congress, the U.S. Attorney General, and the Secretary of the Homeland Security on the best use of criminal intelligence for which interoperability is certainly intertwined.

Recommendation 20 of the Plan encourages all law enforcement agencies to utilize an automated, incident-based criminal records tracking capability, in addition to traditional case management and intelligence systems, to use as an additional source for records management and statistical data.

Recommendation 21 of the Plan identifies the interconnected RISS/LEO (RISSNet and the FBI's Law Enforcement Online) systems as the "initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability. This nationwide sensitive but unclassified communications backbone shall support fully functional, bi-directional information sharing capabilities that **maximize the reuse of existing local, state, tribal, regional, and federal infrastructure investments (emphasis added)**. Further configuration of the nationwide sensitive but unclassified communications capability will continue to evolve in conjunction with industry and the development of additional standards, and the connection of other existing sensitive but unclassified networks."

Recommendation 22 of the Plan identifies interoperability with existing systems at the local, state, tribal, regional, and federal levels with the RISS/LEO communications capability as an immediate priority in order to leverage information sharing systems and expand intelligence sharing.

### **Closing**

Around the nation, tremendous amounts of time, money and effort have been expended in attempts to gather information through the creation of databases. The time has come to shift the focus of effort, technology and funding to connecting what has already been established. Florida supports full implementation of the National Criminal Intelligence Sharing Plan.

Chairman Putnam and Members of the Sub Committee, thank you for the opportunity to have appeared and testified before you today. I can assure you the State of Florida is encouraged by the Sub Committee's interest in facilitating an enhanced information sharing network across the nation. It is our hope that this testimony, and the understanding of Florida's efforts at ensuring a secure and effective network for information and intelligence sharing, will be helpful in your endeavor.