

.....

Strategic Plan

Criminal and Juvenile Justice Information Systems (CJJIS) Council



*Building Enterprise-wide Information
Sharing to Enhance Public Safety,
Improve the Quality of Justice, and
the Efficiency of Operations*

September 2009

Table of Contents

Executive Summary	1
Introduction.....	3
Role of the Criminal and Juvenile Justice Information Systems (CJJIS) Council.....	3
Duties of the CJJIS Council	5
CJJIS Council Committee Structure.....	6
Vision, Mission, Values, Guiding Principles, Core Functions	9
Vision	9
Mission	10
Values.....	10
Guiding Principles.....	11
Core Functions	12
Strategic Issues and Goals	14
Issue 1 Develop a Policy and Planning Framework for Systems Integration.....	14
<i>Goal 1a Develop Operational Scenarios and a Comprehensive Vision of Integrated Justice Information Sharing.....</i>	14
<i>Goal 1b Develop a Scorecard of Justice Information Sharing.....</i>	15
Issue 2 Develop and Expand a Technology Infrastructure for the Sharing of Criminal Justice Information.....	16
<i>Goal 2a Establish and Confirm Positive Identity</i>	17
<i>Goal 2b Expand Access to Information and Determine Legal Status</i>	21
<i>Goal 2c Build Effective and Efficient Information Access & Sharing.....</i>	24
Issue 3: Establish Standards for Data Sharing and Integration	28
<i>Goal 3a Identify the Range of Standards Associated with the CJJIS Council's Vision of Justice Information Sharing.....</i>	29
<i>Goal 3b Research and Adopt, Extend, or Create Standards that will Facilitate Information Access and Sharing</i>	30
Conclusion	31

Strategic Plan

Florida Criminal and Juvenile Justice Information Systems (CJJIS) Council

Executive Summary

Justice and public safety agencies throughout the State of Florida have a critical and enduring need to access and share information at virtually every stage of the criminal justice process. Law enforcement, for example, must quickly and accurately establish the identity of a suspect detained in a criminal incident and determine whether the person is wanted on other charges, represents a danger to the officer or the public, is currently on probation or supervised correctional release, is subject to curfew or geographic restrictions, and a host of other factors in determining the disposition of the encounter—should the suspect be released, cited, or taken into custody? Prosecutors must make charging decisions, Pretrial Service Centers must evaluate and make recommendations regarding the defendant's pre-trial status, Correctional Officers must evaluate and classify those confined, and Judges must make bail, disposition and sentencing decisions all based on information that is available.

Practitioners and key decisionmakers representing all levels and branches of government in Florida have long recognized the need to build integrated information sharing capabilities between justice and public safety agencies and other governmental entities. Through a host of initiatives over the past decade representatives of all levels and branches of government have built and strengthened critical justice information systems and have established much of the foundation necessary to support statewide integrated justice information sharing.

This Strategic Plan of the Criminal and Juvenile Justice Information Systems (CJJIS) Council identifies strategic issues, goals and strategies in building enterprise-wide access and sharing of critical justice and public safety information. The Council's strategic priorities include the development of a policy and planning framework for systems integration, the development and expansion of technology infrastructure and standards for criminal justice information sharing, and enhancing the ability of justice practitioners to establish and verify positive identity, accurately determine a person's legal status, building broad subscription/notification capabilities, federated identity and privilege management, and expanding federated query capabilities to enable timely access to complete information throughout the justice enterprise.

The Council continues to provide strategic oversight and advisory policy direction for the planning, development and operation of the information systems of the Florida Departments of Law Enforcement, Corrections, Juvenile Justice and Highway Safety and Motor Vehicles. The Council also recommends initiatives that will encourage agencies at federal, state and local levels in the public safety sector to coordinate their information technology management programs to maximize the efficient collection, sharing and use of criminal justice data.

Introduction

Justice and public safety officials throughout the State of Florida must be able to access and share critical information at key decision points throughout the whole of the justice and public safety enterprise. Regardless whether the scenario is a police officer conducting a routine traffic stop, a judge setting bail or sentencing an individual in a criminal proceeding, a licensing authority determining the suitability of a person seeking approval to become a day-care provider, or a local merchant determining the qualifications of a person seeking to purchase a firearm, government agencies and, in some situations private industry and the general public, must be able to access and share a broad range of justice information for efficient and effective decisionmaking.

Over the past decade governmental officials throughout the State of Florida have built increasingly robust information sharing capabilities to help meet the day-to-day operational needs of practitioners across all levels and branches of government. These capabilities are rapidly maturing to meet the ever increasing needs of justice and public safety practitioners, as well as mounting demands by the public for greater information sharing and access, accelerating growth in non-criminal justice licensing and employment background investigations, and escalating development of homeland security, intelligence and counter-terrorism information sharing.

This Strategic Plan of the Criminal and Juvenile Justice Information Systems (CJJIS) Council identifies strategic priorities and business objectives in building effective enterprise-wide information sharing, while ensuring privacy and security.

Role of the Criminal and Juvenile Justice Information Systems (CJJIS) Council

The CJJIS Council provides strategic oversight and advisory policy direction for the planning, development and operation of information systems of the Florida Departments of Law Enforcement, Corrections, Juvenile Justice, and Highway Safety and Motor Vehicles. The Council also recommends initiatives that will encourage agencies at federal, state, and local levels in the public safety sector to coordinate their information technology management programs to maximize the efficient collection, sharing, and use of criminal justice data.

The Criminal Justice Information Systems Council was created by the Department of Criminal Law Enforcement Act of 1974 as an advisory body to guide the Florida Department of Law Enforcement's (FDLE) Division of Criminal Justice Information Systems (CJIS) through periodic reviews of its operating policies, procedures and information systems. Since its inception in 1975, the Council has actively addressed the concerns of user agencies at formal public meetings through continuous oversight activities.

The 1995 Legislature expanded the Council's mission and renamed it the Criminal and Juvenile Justice Information System (CJJIS) Council. The CJJIS Council was directed to develop standards and policies that will promote and enhance the sharing of criminal and juvenile justice information throughout the state. The Council was also directed to provide oversight of the data system being developed by the then newly-created Department of Juvenile Justice (DJJ). The Legislature continued to expand the scope and duties of the Council by requiring it to perform a number of additional duties, including oversight of the systems development efforts of the Department of Corrections (DC) and the Department of Highway Safety and Motor Vehicles (DHSMV).

The 2007 Legislature revised the CJJIS Council statutes, amending the duties of the Council and the guiding principles. The CJJIS Council is authorized by Florida Statutes 943.06, as follows:

There is created a Criminal and Juvenile Justice Information Systems Council within the department.

(1) The council shall be composed of 15 members, consisting of the Attorney General or a designated assistant; the executive director of the Department of Law Enforcement or a designated assistant; the secretary of the Department of Corrections or a designated assistant; the chair of the Parole Commission or a designated assistant; the Secretary of Juvenile Justice or a designated assistant; the executive director of the Department of Highway Safety and Motor Vehicles or a designated assistant; the Secretary of Children and Family Services or a designated assistant; the State Courts Administrator or a designated assistant; 1 public defender appointed by the Florida Public Defender Association, Inc.; 1 state attorney appointed by the Florida Prosecuting Attorneys Association, Inc.; and 5 members, to be appointed by the Governor, consisting of 2 sheriffs, 2 police chiefs, and 1 clerk of the circuit court.

Duties of the CJJIS Council

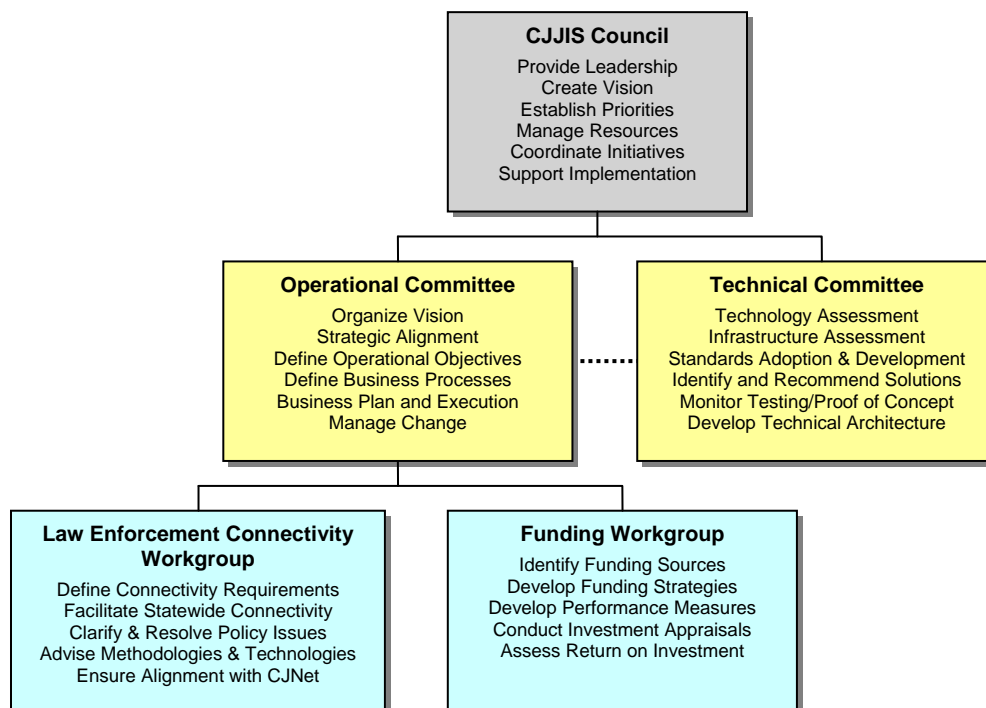
Duties of the CJJIS Council are defined by Florida Statutes 943.08, as follows:

- (1) The council shall facilitate the identification, standardization, sharing, and coordination of criminal and juvenile justice data and other public safety system data among federal, state, and local agencies.
- (2) The council shall adopt uniform information-exchange standards, methodologies, and best practices, applying national standards and models when appropriate, in order to guide local and state criminal justice agencies when procuring, implementing, or modifying information systems.
- (3) The council shall provide statewide oversight and support the development of plans and policies relating to public safety information systems in order to facilitate the effective identification, standardization, access, sharing, integrating, and coordinating of criminal and juvenile justice data among federal, state, and local agencies. The council shall make recommendations addressing each of the following:
 - (a) Privacy of data.
 - (b) Security of systems.
 - (c) Functional and information-sharing standards.
 - (d) Accuracy, timeliness, and completeness of data.
 - (e) Access to data and systems.
 - (f) Transmission of data and information.
 - (g) Dissemination of information.
 - (h) Training.
 - (i) Other areas that effect the sharing of criminal and juvenile justice information and other public safety system information.
- (4) The council shall provide oversight to the operation of the Criminal Justice Network (CJNet) for which the department shall serve as custodial manager pursuant to s. 943.0544. Criminal justice agencies participating in the Criminal Justice Network shall adhere to CJNet standards and policies.

CJJIS Council Committee Structure

The CJJIS Council has established two Committees to focus on specific tasks and strategic priorities in carrying out the duties defined by statute: the Operational Committee and the Technical Committee. The Committees are comprised of Council members and augmented by subject matter experts, technology experts, key stakeholders, and others who will contribute to the work of the Committees. To ensure strategic alignment and effective coordination of activities, the Committees may share some joint members, regularly communicate and periodically meet jointly. In addition, the Committees may establish Workgroups as needed to address specific issues or initiatives. There are presently two Workgroups of the Operational Committee.

CJJIS Council Governance Structure




The **Operational Committee** is comprised of operational practitioners at state and local levels across relevant justice and public safety agencies throughout Florida. This Committee is responsible for organizing the vision established by the CJJIS Council, defining operational requirements and business processes to realize that vision, elaborating scenarios for information sharing, and providing insight and direction in developing business plans for information sharing. This Committee addresses issues and changes that may

need to be made in policy, business practice, and/or statute that will enable justice and public safety agencies to achieve the level of automation and information sharing contemplated in the CJJIS strategic plan.

- **Law Enforcement Connectivity Workgroup:** This Workgroup focuses on building information sharing capabilities for law enforcement agencies at state and local levels throughout Florida. The Workgroup has been tasked with making certain there is a viable statewide system that leverages current efforts of regional partners but is flexible for future needs, including connectivity not only in Florida, but nationally as well. The purpose of this Workgroup is to:
 - Identify and address local law enforcement issues for statewide connectivity;
 - Provide clarification of local policy issues with regard to information sharing;
 - Assist in the development and review of a Request For Information (RFI) to determine the best methodology and associated technology for connecting regional data integration projects; and
 - Ensure statewide data connectivity is consistent with CJNet operations and policy.
- **Funding Workgroup:** This Workgroup focuses on identifying potential funding sources to support for justice information systems and information sharing capabilities (including federal, state, local, and private funding sources) and developing effective funding strategies. The Workgroup develops a unified plan for the sharing of available funding and recommends the plan to the Council for approval. The result is that Florida’s criminal justice agencies do not compete against each other for federal funding; rather, priorities are set and funds are allocated to projects meeting the needs of the criminal justice community as a whole. The Workgroup also addresses performance measures for information sharing, conducting investment appraisals and establishing metrics associated with evaluating return on investment (ROI).

The **Technical Committee** is comprised primarily of technical representatives of participating justice and public safety agencies and supporting IT offices, though one or more operational practitioners may also serve on the Committee to ensure proper understanding of business requirements and context. This Committee is responsible for technical and infrastructure assessments, adopting, extending, and/or creating standards to facilitate information development and sharing, researching and proposing technical solutions, pilot projects, and technical specifications in support of the CJJIS Strategic Plan.

Standards include data modelling (e.g., JIEM), data exchange (GJXDM & NIEM), interoperable communications, fingerprints, photos, technical architecture, etc.



Vision, Mission, Values, Guiding Principles, Core Functions

Vision

Vision statements describe the future business environment and the role of the organization within it.

The CJJIS Council envisions a standards-based, enterprise-wide open-architecture that will enhance public safety and domestic security, improve the quality of justice and the efficiency of operations. Our vision includes eliminating redundant data entry, supporting expanded access and sharing of information, both locally and nationally, for justice and non-justice purposes, and providing timely, accurate, and complete information while respecting the privacy of citizens.

Justice information sharing is envisioned as a statewide architecture that will enable agencies at all levels of government to share information that is already collected and generated in their internal information systems as part of their daily business operations. There is an affirmative expectation that justice and public safety agencies will share information consistent with security and privacy concerns and policies. The architecture will not be designed to share *all* information that an agency may collect, generate and use, but only that information that is appropriate, according to information sharing business requirements the agencies collectively define, and consistent with privacy and confidentiality policies and statutes.

The vision statement recognizes the need to share information at local, state and national levels, for both justice and for non-justice purposes. The CJJIS Council's vision is aligned with the National Strategy for Information Sharing, which outlines a strategy for sharing data with other jurisdictions across the nation, as well as with appropriate Federal agencies.

Our vision also reflects the fact that justice information is increasingly needed for an expanding array of non-criminal justice purposes, such as criminal history checks for licensing and employment, publicly accessible sex offender registries, and other initiatives to ensure the safety of communities and vulnerable populations. As a consequence, we envision that CJJIS planning will align with other information sharing and systems development initiatives at state and local levels throughout Florida.

Finally, our vision reflects our commitment to ensuring the security of our information sharing capabilities. Security will operate at several levels to ensure that only authorized users will have access to the system, and only for authorized purposes. Justice information sharing will operate to enforce effective security through rigorous policy and technology, including user authentication, monitoring operations, auditing transactions, and disaster recovery planning.

Mission

Mission statements identify the overall purpose for which the organization is organized and how it operates. The CJJIS Council, as the governance structure demonstrates, represents justice, public safety and governmental officials at all levels and across all branches of government.

The mission of the CJJIS Council is to provide statewide oversight, coordinate criminal and juvenile justice information among federal, state, and local agencies and relevant partners, and support the development of plans and policies to enable positive identification, broad information sharing and interoperability, while recognizing the independence of each agency and ensuring security, privacy and confidentiality.

The mission statement underscores the collaborative nature of justice information systems planning, design, development and implementation. No single agency is directing the effort; rather, all participants are working together to develop enterprise-wide information sharing for common objectives. It is this collaborative and coordinated planning and development that serves as an important foundation to our on-going work.

Values

The CJJIS Council has formulated a series of values which guide and direct planning efforts for justice information sharing. These values are enumerated below.

- Quality of Life*** The residents and visitors of Florida should enjoy a high quality of life and feel safe and secure in their homes, on their streets, in their neighborhoods, and throughout the community;
- Efficiency*** Integrated justice information sharing will improve public safety and homeland security, enhance the effectiveness of decisionmaking and operations, and achieve great efficiency and return on investment (ROI).

<i>Fairness</i>	The justice system should be fair to all parties, respecting the constitutional rights of defendants, and ensuring protection of the rights and privacy of victims and the public.
<i>Public Trust</i>	We will provide services that contribute to public trust and confidence in the justice system.
<i>Data Quality</i>	Eliminating duplication of effort in capturing data across information systems will improve the timeliness, accuracy and completeness of information, and facilitate informed decisionmaking and greater cost-efficiency of operations.
<i>Collaboration</i>	We will seek opportunities to collaborate and cooperate with justice and justice-related organizations at all levels of government and related partners to enhance the performance of the justice system as a whole.
<i>Independence</i>	We acknowledge both the independence of justice and justice-related organizations, as well as the interdependence of their operations—no one justice organization can operate effectively without the cooperation of the others.
<i>Accountability</i>	We accept responsibility to be accountable for the performance of the justice system and for proper stewardship of public funds and other resources.
<i>Sense of Timeliness</i>	We are committed to the achievement of our mission and cause and as such we will respond to information sharing requests in a deliberate manner.

Guiding Principles

The CJJIS Council has drafted a set of principles which have been codified into Florida law as Florida Statutes s. 943.081. The principles are designed to guide the Council and participating agencies in their planning, development, and implementation of information systems and justice information sharing efforts statewide.

The following guiding principles adopted by the Criminal and Juvenile Justice Information Systems Council are hereby adopted as guiding principles for the management of public safety system information technology resources:

- (1) Cooperative planning by public safety system entities is a prerequisite for the effective development of systems to enable sharing of data.
- (2) The planning process, as well as coordination of development efforts, should identify and include all principals from the outset.
- (3) Public safety system entities should be committed to maximizing information sharing and moving away from proprietary positions taken relative to data they capture and maintain.
- (4) Public safety system entities should maximize public access to data and, in so doing, should specifically implement guidelines and practices that address security, privacy, and confidentiality.
- (5) Public safety system entities should strive for electronic sharing of information.
- (6) The practice by public safety system entities of charging each other for data should, insofar as possible, be eliminated. Further, when the capture of data for mutual benefit can be accomplished, the costs for the development, capture, and network for access to that data should be shared.
- (7) The redundant capture of data should, insofar as possible, be eliminated. Redundant capture of data should be discouraged unless there is a specific business need for it.
- (8) Public safety systems should adhere to information-exchange standards approved by the council.
- (9) The council should adopt where possible applicable national standards for data exchange.

Core Functions

Integrated justice information sharing initiatives are typically designed to provide the following core functions:

- ***Universal or Federated Query*** of multiple local, regional and national information systems. Users should be able to initiate a single query that is capable of accessing multiple information systems and returning results. The user should have the ability to query all systems to which they have authorized and authenticated access, as well as the ability to specify a sub-set of systems that will be interrogated for the query.

- **Push** information electronically to another agency/system based on actions taken within the originating agency. Data should be electronically pushed (based on business rules that have been mutually agreed and specified) to the information sharing architecture for subsequent sharing with other authorized agencies and systems, rather than having users exchange information in paper or other manual methods.
- **Pull** information from other systems for incorporation into the recipient agency system. Users should be able to pull automated information from other agencies and systems for incorporation into their internal systems rather than having to re-type it, while ensuring security mechanisms are in place to retain its exemptions on confidentiality.
- **Publish** information regarding people, cases, events and agency actions. The information may be published to internal agency information systems, the information sharing architecture, or other systems for subsequent access by authorized users.
- **Subscribe** to a notification service. Users should be able to subscribe to notification services that will automatically notify them (via e-mail, pager, etc.) of significant events regarding individuals, cases and agency actions. Probation officers, for example, should be able to subscribe to automated notification of a subsequent arrest of every probationer assigned to their caseload. Similarly, other justice and governmental representatives should be able to subscribe to notification of significant events (e.g., arrests, convictions, sentencing, correctional release) regarding individuals and cases.

Strategic Issues and Goals

The CJJIS Council's previous strategic plan, *Improving Criminal and Juvenile Justice Information for the 21st Century; Information Resource Strategic Plan 2007-2010*, identified three strategic issues:

1. Development of a policy framework for systems integration;
2. Development and expansion of a technology infrastructure for the sharing of criminal justice information; and
3. Establishment of standards for data sharing and integration.

These strategic issues, which largely originate from the statutory duties of the CJJIS Council, are persistent and will continue to structure much of the work of the CJJIS Council.

Strategic Issue 1: Develop a Policy and Planning Framework for Systems Integration

Effective justice information sharing requires a comprehensive and enduring policy and planning framework. Just as technology continues to evolve and mature, so do the operational needs of justice and public safety practitioners. The policy and planning framework needs to provide agility in addressing emerging requirements for expanded access and information sharing from justice and public safety practitioners, the legislature, federal agencies, private industry, and the general public.

Strategic Goal 1a

Develop Operational Scenarios and a Comprehensive Vision of Integrated Justice Information Sharing

Develop operational scenarios of integrated justice information sharing (IJIS) across the whole of the justice and public safety enterprise. These scenarios articulate in operational terms the nature and business value of justice information sharing.

Scenarios describe the business context of events, incidents, or circumstances in which information must be exchanged between agencies and/or domains. For example, the scenario may address adult felony case processing, from the call for service through law enforcement reporting, arrest, prosecution, judicial processing, adjudication, sentencing, community supervision or correctional confinement, discharge, supervision, etc. Careful elaboration of operational scenarios will identify critical points at which information must be shared between agencies and units of government for efficient operations, effective service delivery, informed decisionmaking, and enhanced public safety.

Scenarios can be used to depict current (i.e., “as is”) information exchange practices among participating agencies, thereby identifying gaps, impediments, and other flaws in business processes and data exchanges. They can also be used to characterize potential future (i.e., “to be”) environments that envision broader and more expansive information sharing, as well as changes in business practice.

Once information sharing scenarios have been created, operational requirements are identified and a comprehensive vision of justice information sharing is created. The vision provides an operational view of justice and public safety information sharing.

Strategies

- 1.1 Develop operational scenarios for justice information sharing addressing primary justice business cases (i.e., adult felony, adult misdemeanor, juvenile justice case processing) in facilitated workshops with operational practitioners and business subject matter experts (SMEs). The scenarios will reflect the “to be” information sharing capabilities that justice and public safety practitioners desire to achieve throughout the criminal justice enterprise.
- 1.2 Define operational requirements and develop a comprehensive vision for justice information sharing throughout Florida based on a review and analysis of the scenarios that are developed. While the scenarios are detailed descriptions of operational information sharing capabilities for fundamental business cases, the comprehensive vision looks across the scenarios and provides an enterprise-wide view of information sharing.

Strategic Goal 1b

Develop a Scorecard for Justice Information Sharing

An assessment of the extent to which information can be accessed and shared across the whole of the justice and public safety enterprise, as described in the IJIS scenarios produced in Strategic Goal 1a, will enable the CJJIS Council to create a scorecard to assess the status of statewide criminal justice information access and sharing capabilities. The IJIS scorecard will assist the Council in identifying gaps and impediments to information sharing and will help in determining the source of the gap or impediment. Some information sharing, for example, may be hindered by the lack of automation among key agencies, or perhaps the failure to automate specific data or to share it in an open systems standard format that would enable other agencies to properly interpret and accept the information.

Armed with a clear vision of justice information sharing, well defined scenarios that articulate the operational context and business value, and scorecards assessing the nature and source of gaps and impediments to achieving the level of information sharing envisioned, the Council will be better able to prioritize programs that will provide the greatest return on investment.

Strategies

- 1.3 Develop a scorecard for justice information sharing based on the comprehensive vision and operational scenarios. The scorecard articulates operational requirements and performance metrics for justice information sharing and it enables the CJJIS Council to measure the extent to which existing operations meet strategic priorities.
- 1.4 Conduct gap analyses to identify and evaluate differences between the information sharing capabilities envisioned in the scenarios and current operations and planned projects. In addition, the gap analyses will assess the nature and causes of these variances, and describe actions that can be taken (e.g., changes in business practice, adoption of new or emerging technologies, expansion of infrastructure, coordinated planning, etc.) in order to ameliorate or close the gaps, enabling the CJJIS Council to prioritize projects and initiatives to achieve the greatest return on investment.

Strategic Issue 2: Develop and Expand a Technology Infrastructure for the Sharing of Criminal Justice Information

Justice practitioners throughout the State of Florida have an expansive array of information systems at their disposal to assist them in completing their myriad responsibilities each day. Most law enforcement agencies have automated records management systems, computer-aided dispatch, access to statewide and national systems and information resources (e.g., CCH, FCIC, NCIC, NLETS, etc.) through CJNet. Similarly, prosecutors, probation and parole officers, correctional facilities and court officials (both clerks and judges) have an array of automated case management information systems and access to state and national resources to meet many of their fundamental day-to-day business needs.

The State has made significant investments in building statewide infrastructure and statewide information systems and resources, including AFIS, CCH, Sex Offender Registry, Career Criminal Registry, Comprehensive Case Information System (CCIS), Judicial Inquiry System, Live Scan Fingerprint capture stations, etc. These systems provide an enviable level of information resources to justice and public safety practitioners throughout Florida, as well as the general public and private industry.

Despite the significant advances the individual agencies, regions, and the state have made, however, there are gaps in existing systems and enduring operational issues that must still be addressed in building robust information systems and enterprise-wide information sharing. Justice practitioners, state and local justice agencies, and the CJJIS Council are actively planning and building projects to address these gaps in information sharing capabilities.

Three strategic goals have been identified by the CJJIS Council:

- a. Enhance public safety by establishing and confirming the positive identity of persons with whom we are dealing at every stage of the justice process.
- b. Improve the quality of justice and the effectiveness of decisionmaking by expanding access to available information and enabling users to determine the legal status of persons with whom we are dealing at every stage of the justice process.
- c. Building more effective and efficient capabilities to access, analyze, and share information between agencies and jurisdictions throughout the State of Florida and beyond.

***Strategic Goal 2a
Establish and Confirm Positive Identity***

When a law enforcement officer makes a routine stop—traffic or otherwise—something that occurs hundreds or perhaps thousands of times each and every day throughout Florida, in nearly every community throughout the state, and in every state throughout the nation and even around the globe, their first objective is usually to determine the identity of the person with whom they are dealing.

- Does the person have a valid and appropriate license or other photo-based state issued identification card?
- Is the person (and the vehicle, in a traffic stop) wanted in this or another jurisdiction?
- Does the person pose a danger to the officer or to society?
- Do they have a record of criminal behavior that may have relevance to the current situation—for example, is the person on probation with curfew restrictions or have they been convicted of driving while intoxicated (DWI) with conditions that they may only drive to and from their place of employment?

If the person does not have a valid driver's license or other photo-based state identification card, the officer may not be able to accurately determine their

identity. A wanted person may, in such a situation, elude apprehension. If the person does have a driver's license or other state ID, the officer can compare the photo on the document with the appearance of the person with whom they are dealing and normally make a reasonable determination of whether the person is who they claim to be.

Identity is usually established with biometric precision. When a person is arrested their fingerprints are taken and compared with other fingerprints on file. Arrested persons' fingerprints are compared automatically to all fingerprints stored in the state's Automated Fingerprint Identification System (AFIS). If there is no match, a follow-up name search is conducted to identify potential subjects whose prints are stored on microfilm. If identical fingerprints are discovered in an existing record, fingerprint examiners will verify the identity, and the existing criminal history is updated with the new arrest information, including any different names (or variations of the subject's name) that were reported. If there is no record of prior arrest a new state identification number (SID) is assigned, a new record is created, and the fingerprints captured at arrest are added to the AFIS. Much of this process is now greatly expedited through the use of AFIS and Livescan fingerprint capture work stations.

Not all people involved in the criminal justice system, however, are fingerprinted. If a person is not arrested or booked, but merely cited and released, no fingerprints will be available to verify identity when the case is brought before the court. In such cases, the Comprehensive Case Information System (CCIS) assigns a unique identifier which can be used to relate cases to individuals. This unique identifier is contrived by using demographic and other information that is sent to CCIS and compared to other stored data. A sophisticated algorithm is used for this comparison and a unique Identifier is assigned to the individual. This unique identifier is then stored and future cases are tied to the individual.

Establishing and confirming the identity of the person with whom we are dealing is a critical requirement at virtually every stage of the criminal justice enterprise. Jailers must know who is in their facility and ensure that they hold and release the correct person. Judges must know with certainty that the person appearing before them is in fact the defendant. Probation officers must know the identity of persons on their caseload and verify that identity when the client provides samples for random drug screening.

Several initiatives are presently underway in Florida to address this strategic goal.

1. Florida's Integrated Criminal History System—FALCON—is a state-of-the-art system capable of collating information from multiple sources, identifying criminal suspects, and reporting data. It will improve and expand positive biometric identification directly to the end user and ties a criminal's identification—with fingerprints—to a computerized criminal history (CCH), which will be more complete and easier to understand. It will also enable the comparison of palm prints and dynamic image management. Implementing the capability to store and process palm prints as well as searching latent fingerprints against all prints, including non-criminal as allowed by state and federal laws, will increase the probability of subject identification and help solve crimes. Moreover, it will be integrated, with the ability to pull information from state and national databases
2. FALCON also supports the Rapid ID program. Small, relatively inexpensive, one to four-finger fingerprint capture devices are used to either validate a subject's identity, using one finger and subject demographic information (such as State ID), or search and identify a subject, using only the subject's two fingers.
 - a. Sheriffs' Offices can biometrically confirm the identity of sex offenders at the time they report for re-registration, as required by the Jessica Lunsford Act.
 - b. Department of Corrections Probation Officers can biometrically confirm the identity of probationers at the time they report for supervision.
 - c. Court Rooms can confirm the identity of the defendant and automatically obtain Florida criminal history records and Hot File data (i.e., wanted person records and status records) whenever a person appears in court.
 - d. Jails can confirm the identity of prisoners prior to dispensing medications or releasing prisoners from confinement. The Pinellas County Jail is identifying subjects for every situation in which confirmed identity will affect the outcome at booking or termination of custody.
 - e. Patrol Vehicles can quickly confirm or determine the identity of a person and whether they have a Florida criminal history or an active warrant prior to issuing a notice to appear. Florida Highway Patrol is testing the use of Rapid ID during roadside stops.
 - f. FDLE Regional Offices have fingerprint capture devices available for use by local agencies interested in testing the use of Rapid ID technology in special operations.
3. Facial recognition software uses computer technology to analyze and compare digital images for the purpose of identifying offenders when

their identity is otherwise unknown. Because the human face contains many unique physical characteristics, facial recognition technology analyzes the facial image, measuring characteristics such as the distance between eyes, the length of the nose, and the angle of the jaw. The technology converts an image into digital code, or a face-print, and compares it against existing facial codes in a database. Facial recognition software produces a score and displays images that most closely match the face-print and any known characteristics. Users are then able to review the potential candidates and make a final determination on whether there is a match. Facial recognition software is typically used as an investigative tool and to confirm a person's identity, not for positive identification.

Facial recognition technology will become part of the FALCON implementation as the initiative progresses. In addition, the Pinellas County Sheriff's Office has implemented a facial recognition solution which is used in booking, correctional release, inmate management, law enforcement investigations, airport passenger screening (to check each ticketed passenger against a database of known terrorists and wanted felons), jail visitation (to determine whether a jail visitor is a wanted felon), and in the Criminal Court Complex (to check each visitor against a database of know felons).

4. Digital mugshots and driver license photos can be shared and available remotely to justice practitioners to aid in verifying identity and to combat identity theft. Digital photographs captured by the Division of Highway Safety and Motor Vehicles (DHSMV) are presently accessible by law enforcement. Digital mugshots are presently available for sex offenders, from Department of Corrections, and will be submitted to FALCON as part of the electronic arrest record together with fingerprints.
5. DNA Confirmation will enable courts and corrections to confirm whether a DNA sample is already on file for an offender. This confirmation will prevent the costly collection and processing of multiple DNA samples for the same subject.

Strategies

- 2.1 Monitor the development and implementation of FALCON, and incorporate in tactical planning and development as appropriate
- 2.2 Monitor and support the development, implementation and expansion of the Rapid ID program to facilitate identification and identity verification by justice practitioners statewide, and incorporate in tactical planning and development as appropriate.

- 2.3 Monitor the development, implementation and expansion of facial recognition technology, and incorporate in tactical planning and development as appropriate
- 2.4 Monitor the development, implementation and expansion of initiatives to share mugshot and driver license photos, and incorporate in tactical planning and development as appropriate.
- 2.5 Monitor the development and implementation of DNA confirmation to enable courts and corrections to confirm whether a DNA sample is already on file for an offender.

Strategic Goal 2b

Expand Access to Information and Determine Legal Status

Justice and public safety practitioners throughout Florida need access to a broad variety of information systems and resources beyond their own internal agency applications in order to do their jobs effectively. Just as we must know the identity of the person with whom we are dealing at every stage of the criminal justice process, we also need to know their current legal status and perhaps changes in that status. Justice agencies will want to know, for example, whether the person with whom they are dealing is wanted on active warrants in this or other jurisdictions. Licensing authorities will want to know if a person who holds a license to provide day care for children, for example, is arrested for a disqualifying offense in this or another jurisdiction. Probation and parole officers want to know immediately when one of their clients is arrested anywhere in the state, and perhaps in other jurisdictions.

Warrant information should be immediately available to authorized users to ensure that wanted persons are properly identified and appropriately dealt with. Too often warrant information is processed manually or typed and re-typed in agency applications. These practices retard the timeliness of the information and provide opportunities for inadvertent errors in data entry. Without access to accurate, timely and complete warrant information, justice practitioners may come into contact with a wanted person and not even know it, perhaps jeopardizing their safety and missing an obvious opportunity to apprehend a fugitive.

Creating statewide watch lists and providing automatic notification of arrest or other significant change in a person's legal status are important capabilities to ensure public safety and enhance the quality of justice decisionmaking. Licensing authorities must be notified immediately if a person who holds a sensitive license is arrested for a potentially disqualifying offense. Similarly, key public agencies (justice agencies, Department of Education, etc.) need to be notified immediately if one of their employees is arrested any where in the

state, and beyond. Simply providing access to key justice resources is insufficient, as that would require users to constantly query different systems to determine any change in the legal status of interested parties.

Local law enforcement agencies also need to be able to share crime and investigative information with each other statewide. Offenders are quite mobile and may be involved in criminal activities in numerous local jurisdictions across the state and in even in adjoining states. Law enforcement should have the ability to access, analyze, and share critical information with other investigative agencies within their region and across the state.

Several initiatives are presently underway in Florida to address this strategic goal.

1. Florida is participating in the National Warrants Task Force, sponsored by the Federal Bureau of Investigation, and is currently engaged in a feasibility study for creation of electronic warrants. Effective warrant processing will make uniform information immediately available to justice practitioners throughout the state of Florida as well as nationwide, with links to FCIC and NCIC.
2. Lee County is presently testing an active warrant alert calendar system. The purpose of the system is develop and implement an automated computer program to provide an “active” link between NCIC/FCIC warrant information systems (and other information retrieved by the Judicial Inquiry System or JIS) and the calendar information from the Comprehensive Case Information System (CCIS) to alert the Sheriffs Department, State Attorneys Offices and court agencies of criminal defendants appearing at arraignment or other pretrial events with an active criminal warrant in advance of the hearing.
3. Another component of FALCON is the capability to create watch lists and providing automatic notification of arrests for both criminal subjects and retained applicant fingerprints.
 - a. For criminal subjects, investigators can identify persons of interest (creating an individual watch list). All fingerprint supported arrests that are reported to FDLE will be searched against the fingerprints of persons identified in watch lists. Notification of a subject’s arrest will be sent to subscribing users.
 - b. For retained applicants, all incoming arrests will be search against the retained fingerprints of applicants. Notification of an applicant’s arrest will be sent to the applicant’s employer.
4. Various law enforcement regional data integration projects are currently under development in Florida. These projects, working in

conjunction with the state's seven Regional Domestic Security Task Forces, share law enforcement information between sheriffs' offices and police departments within their region.

The seven projects and an eighth state law enforcement data node will be connected together by the Florida Department of Law Enforcement into a single, statewide data sharing system. The system, coined the Florida Law Enforcement eXchange (FLEX) will provide law enforcement across the state the ability to quickly and easily access and analyze the thousands of records found in individual city, county and state law enforcement agencies records management systems. FLEX is currently in development at the state level.

Information such as local field interview reports, pawn data, incident, dispatch and offense information will for the first time be searchable by agencies outside of the agency of ownership and provide instant access to law enforcement officers from Pensacola to Key West.

The state has adopted a regional concept of information sharing. Each region has an information sharing project that will be incorporated into the statewide data sharing project. Three regions and the State node did not have dedicated projects in progress, and instead opted to jointly procure a single user interface with data analysis tools. This effort is referred to as the Regional Law Enforcement eXchange (R-LEX) project, which is a subset of FLEX. The state system is designed to link the regional projects and fusion centers to facilitate information sharing at the state level and provide the ability to share information at the federal level.

Strategies

- 2.6 Continue to participate in the National Warrants Task Force and the feasibility study for the creation of electronic warrants. Review and assess policy and legislative implications, operational considerations, and technological solutions to support the creation and management of electronic warrants and effective warrant processing, and incorporate in tactical planning and development as appropriate.
- 2.7 Monitor and assess the active warrant alert calendar system being piloted in Lee County, assess operational and technical requires regarding future development and expansion to other jurisdictions statewide, and incorporate in tactical planning and development as appropriate.
- 2.8 Monitor and support the development, implementation and expansion of the watch lists and subscription notification capabilities of FALCON.

- 2.9 Continue to monitor and support the development and implementation of R-LEX and FLEX, and incorporate in tactical planning and development as appropriate.

Strategic Goal 2c

Build Effective and Efficient Information Access & Sharing

Integrated justice information sharing programs improve the quality of information and the quality of decisions, by eliminating error-prone redundant data entry. In addition, by sharing data between systems, information sharing typically improves the timely access to information, a critical factor at many justice decision points. Integrated justice efforts enable the sharing of crucial information without regard to time or space; multiple users can access the same records simultaneously from remote locations around the clock.

Integration also substantially improves the consistency and reliability of information, and enables immediate access by key decisionmakers. Errors in justice information can be greatly reduced by eliminating redundant data entry, which not only results in lower labor costs, but also significantly improves the quality of justice decisionmaking.

Building integrated justice information systems does not mean that all information between agencies is shared, without regard to the event, the agencies involved or the sensitivity of the information available. Rather, agencies need to share critical information at key decision points throughout the justice enterprise.

Some information contained in documents that are shared between agencies is the same, e.g., information regarding the defendant, the victim, the circumstances of the offense, the time, date and location of the incident, the arresting officer, etc. In spite of the commonality of this data, too often it must be re-entered into multiple independent agency information systems.

In addition to the time and effort expended by agency staff to process and automate this duplicate information, there is inevitably delay in making information available to users. These delays in processing represent more than the simple administrative burden to the responsible agency—they also raise the specter of flawed decisionmaking based on incomplete or outdated information.

To exacerbate the situation, every time a person enters data into an automated system they have an opportunity to inadvertently make an error—press the wrong button, misinterpret a figure, overlook a piece of information, or innocently transpose letters or numbers. Justice officials may make

consequential decisions regarding the arrest, bail, sentencing, or release of a person based on inaccurate or inadequate information.

Justice practitioners throughout the state of Florida have access to a broad array of different information systems and resources. Often, however, the security protocols for accessing these systems require the user to create a separate user name and password for each system. The net result is that many users have multiple user names and passwords, and keeping track of all of the different user names and passwords and which systems they correspond to becomes a challenge.

It is not entirely uncommon to see post-it notes attached to computer monitors with user names and passwords written down, or perhaps an index card with all of the pertinent user names and passwords discretely hidden below the monitor. Such efforts undermine the security of information systems and networks, and waste time and effort at a time when both are scarce. Users are increasingly demanding single sign-on capabilities that will authenticate the identity and authorization of the user and enable immediate access to multiple systems.

The Global Federated Identity and Privilege Management (GFIPM) framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. The concept of globally understood metadata across federation systems is essential to GFIPM interoperability. Just as a common Extensible Markup Language (XML) data model was the key to data interoperability, a standard set of XML elements and attributes about a federation user's identities, privileges, and authentication can be universally communicated. The GFIPM metadata and framework support the following three major interoperability areas of security in the federation:

- Identification/Authentication—Who is the end user and how did they authenticate?
- Privilege Management—What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?
- Audit—What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?

The GFIPM Metadata specification is being used in a limited pilot capacity today. Lessons learned and feedback from this pilot were incorporated into the public release of the GFIPM Metadata specification, which is available from

the Global Justice Information Sharing initiative of the U.S. Department of Justice.

A corollary requirement for effective justice information sharing is the ability of users to initiate a universal or federated query. Rather than conducting independent searches for relevant information across multiple data sources, a federated query enables the user to enter the information once and interrogate multiple information sources simultaneously. Federated queries typically allow the user to search all or only selected data sources from the universe of sources that are available and for which the user is authorized. The results of the federated query are usually built dynamically and consolidated, so the user has a comprehensive picture of the individual who was the subject of the search.

Several initiatives are presently underway in Florida to address this strategic goal.

1. The Comprehensive Case Information System (CCIS) is a secured Internet Portal which provides single point of access for statewide court case information. CCIS, which is provided and maintained by the 67 Clerks of Court across Florida, enables broad person and case searching capabilities providing names, cases, case number and status, statute and statute text, demographics, sentencing data, financial information (fines, fees and costs), outstanding and served warrants, summons and capias information, progress dockets and document images. In addition CCIS provides the capability of providing the unique person identifier as well as a sexual offender/predator search and notification system
2. The Judicial Inquiry System (JIS) is a technology initiative by the State Courts which offers the Judiciary and other criminal justice entities access to a streamlined dashboard in which a user may query multiple data sources through a single point of entry. The JIS consists of two distinct applications: JIS Search, through which individual queries are performed, and the JLA First Appearance Calendar, which creates an automated docket of merged data source responses for arrestees in each county every day. The JIS does not warehouse any information, but instead provides only the mechanism through which users may query current data, allowing each source to retain control over individual database content. The system is constantly evolving to accommodate the current and future needs of the Courts.

JIS accesses many criminal justice data sources providing the following information:

- FCIC and NCIC criminal histories
 - Hotfiles (Warrants, Injunctions, Probation Status, Risk Alerts – HRSO, VFOSC, Sex Offender, Career Offender, Immigration Violator, etc.) found in both FCIC/NCIC
 - Florida Driver and Vehicle Information via DHSMV’s DAVID system
 - Out of State Driver Histories via NCIC
 - Current incarceration information from Justice Exchange via APPRISS
 - Inmate Database and Supervision statuses from the Department of Corrections
 - Juvenile Arrest and Disposition information via Department of Juvenile Justice
 - Case numbers, case charge statutes, status and disposition history, progress dockets, and event calendars via the Clerks of Court system CCIS.
3. **FACTS:** The goal of FACTS is to improve the effectiveness of law enforcement personnel when investigating criminal and terrorist activities by querying available criminal and public record databases to determine potential associations that might generate investigative leads. The purpose of the FACTS system is to provide a hardware and software infrastructure to enable agency staff access to information that can “connect the dots” by providing more detailed and accurate information regarding persons and vehicles involved in incidents and criminal activities. The use of FACTS should also facilitate collaboration among staffs within and among agencies.

FACTS does not provide access to law enforcement data such as pawn data that is maintained by local law enforcement agencies. FACTS provides access to law enforcement data that is currently submitted from local agencies to the state: criminal history, corrections, and sex offender data. FACTS does not store intelligence data; it only accesses public record data and Florida law enforcement, driver license, and motor vehicle data to develop potential investigative leads. This data originates from the state's databases and from Seisint's (now Lexis/Nexis) public record database. All of the Florida’s data remains under the control of the State and is not disseminated out of its jurisdictional areas.

The statewide information consists of five datasets collected and maintained by Florida state agencies:

- Criminal history information,

- Department of Corrections information with photo images,
- Sexual offender/predator criminal history files,
- Driver license information with images, and
- Motor vehicle registration information.

The Seisint (now Lexis/Nexis) public records database consists of the following datasets:

- Pilot licenses issued by the Federal Aviation Agency
- Aircraft ownership
- Property ownership
- U.S. Coast Guard-registered vehicles
- State sexual offender lists
- Corporate filings
- Uniform Commercial Code filings or business liens
- Bankruptcy filings
- State-issued professional licenses
- Internet domains
- Hunting and Fishing licenses
- Firearms and Explosive permits
- DEA controlled substances licenses
- Residential and Business Phone listings
- Civil courts records
- Persons and Businesses identified by various organizations
- State Department of Corrections' court and arrest records and photos (when available)

Strategies

- 2.10 Research and assess policy issues, operational requirements, technical solutions, national standards and industry best practices to facilitate single sign-on, federated identity and privilege management, and federated query capabilities to support justice information sharing, establish priorities, and incorporate in tactical planning and development as appropriate.
- 2.11 Continue strategic and tactical planning efforts which identify and prioritize projects that will create, expand and enhance integrated justice information sharing.

Strategic Issue 3: Establish Standards for Data Sharing and Integration.

Building truly enterprise-wide information sharing capabilities requires a robust and dynamic technology infrastructure that will support justice and public safety practitioners at all levels and branches of government. The technology architecture for justice information sharing should align with the

information technology investments the State is making in other domains, as well as emerging national standards and industry best practices.

Information sharing standards enable different information systems to exchange information irrespective of the technology being used. National information sharing standards, such as the National Information Exchange Model (NIEM), are actively being developed and implemented in federal, state, and local jurisdictions throughout the nation. These standards leverage current information technology investments, facilitate improved and expanded information sharing, and provide the operational agility to respond to the evolving needs of a changing world.

Strategic Goal 3a

Identify the Range of Standards Associated with the CJJIS Council's Vision of Justice Information Sharing

A host of standards are potentially applicable to justice information sharing. Potential standards include data modeling, data exchange, interoperable communications, fingerprints, facial recognition, iris scanning, photographs, technical architecture, security, federated identity and privilege management, etc.

An initial assessment of the range and scope of standards that are associated with information sharing capabilities, as defined by the IJIS vision and the strategic priorities established by the Council, will enable the Technical and Operational Committees to assess the status of standards development and maturity in each area. AFIS fingerprint image standards, for example, are robust and accepted by both the field and private industry solution providers, as are document imaging standards. Data exchange standards, such as NIEM, are progressing and Florida has an opportunity to adopt and extend these standards, as well as influence their development through participation in key NIEM committees.

Strategies

- 3.1 Develop an inventory of standards that are associated with information sharing capabilities defined by the vision and strategic priorities of justice information sharing as established by the CJJIS Council. The inventory should:
 - 3.1.1 Identify the nature of the standards,
 - 3.1.2 Discuss the relevance, applicability and business value of the standards to the justice information sharing priorities established by the CJJIS Council,

- 3.1.3 Review the status, maturity, industry adoption and future direction of the standards, and
- 3.1.4 Assess Florida's current or planning adoption and/or use of the standards.

***Strategic Goal 3b
Research and Adopt, Extend, or Create Standards that will Facilitate
Information Access and Sharing***

Once the range and scope of standards for information sharing have been identified, and research is completed regarding the nature, maturity, and applicability of the standards, the CJJIS Council will be able to make decisions regarding the adoption, extension, or creation of specific standards that will facilitate integrated justice information sharing and access. Work should begin in earnest to adopt, extend or create standards that will facilitate information sharing between justice and public safety agencies at all levels of government.

- 3.2 Develop a tactical plan for the adoption, extension, or creation and use of specific standards that will facilitate or enable integrated justice information sharing and access.

Conclusion

This Strategic Plan of the Florida CJJIS Council identifies strategic issues, goals and strategies in building enterprise-wide access and sharing of critical justice and public safety information. The Plan, which is *business-driven* and *technology enabled*, is designed to build information access and sharing among both justice and non-justice agencies and users.

The CJJIS Strategic Plan establishes a foundation to guide continuing work in building a statewide information sharing infrastructure, expanding and enhancing operational information systems among participating agencies, defining information sharing standards and services, and improving business operations for effective operations and decision making at all levels of government.

Planning and development activities will be structured to leverage the considerable level of justice information sharing already achieved by state and local justice agencies throughout the State of Florida. In addition, the plan envisions short-term pilot implementations and projects designed to build incremental change and demonstrate the operational value of expanding access and information sharing. Given the existing economic climate and the scarcity of financial resources, short term projects that demonstrate the tangible business value of effective information sharing will be a priority.