FEDERATED IDENTITY AND SHARING CRIMINAL JUSTICE INFORMATION

SEARCH MEMBERSHIP MEETING
July, 2011 St. Louis, Mo.

David Gavin
“However beautiful the strategy, you should occasionally look at the results..”

--Winston Churchill
You've got to be very careful if you don't know where you are going, because you might not get there."

-- Yogi Berra
1. Agencies’ Responsibilities Drive
Local law enforcement agencies are actively looking to find or improve ways to fulfill their responsibilities to:
   1. Take advantage of all tools possibly available;
   2. Share their data with other agencies for mutual benefit

State, tribal, and federal agencies are actively looking to find or improve ways to fulfill their corresponding responsibilities.
2. **Real Successes Affirm**
The job is far from done, but real successes are occurring at the local, state, tribal, and federal level.

3. **The Economy Directs**
Sufficient strategies and solutions that are less expensive will prevail in the long run, especially at the local level.
4. Leadership Determines

The combination of all factors drives the Information Sharing Environment to its future destination. It is critical to:

- Identify and act upon those factors that can be managed;
- Anticipate and prepare for those that cannot.
Warning Words from Leading Chiefs of Police

“If we are not careful, police will lose touch with the community again, we will lose control of our public spaces again, and we will witness a return to the disorderly conditions and high crime rates that have largely faded from memory. Worst of all, we may disable the capacity of local police departments to ‘connect the dots’ and prevent the next terrorist attack...”

Chief Mark Marshall, President, IACP, and
Chief William Bratton, LAPD
N. Y. Daily News, May 23 2011
Information Sharing Environment (ISE)

Reinventing the Public Safety Business Model

Sustaining and Enhancing State, Local, and Tribal Information Sharing Capacity in the Current Fiscal Environment

“Thought Document” from ISE
The reality of these (fiscal) cuts is resulting in a willingness on the part of public safety executives to consider a new public safety business model.

There are a myriad of existing assets and efforts underway...with the potential for break-through gains if effectively integrated.
Reinventing Public Safety Model
ISE Perspective

By offering to facilitate strategic planning and collaboration, and better leveraging and aligning current efforts under this strategic framework, the Federal government could partner with national public safety and law enforcement officials and Reinvent the Public Safety Model for the 21st century.
Reinventing Public Safety Model
ISE Solutions

- Shared Services and Computing
- Dedicated Public Safety Network
- Proven Policing Strategies
- Information-Led Productivity Gains
- Leveraging Collective Demand
Shared computing exists today in many different formats. Well-known companies such as Google, Amazon, and Yahoo have pioneered shared, or “cloud”, computing models.

This model provides many benefits to individuals using a shared, integrated platform.

Agencies can also store and access information through the shared, integrated platform in an encrypted form with controlled access to that information according to administrator-defined rules and designations.
Reinventing Public Safety Model

Shared Services

- Examples
  - CJIS Systems
  - NLETS
  - RISS
  - HSIN
  - LEO
  - OneDOJ
  - LInX
  - N-DEx
Shared Services

□ Assured SBU/CUI Network Interoperability Initiative

□ Responding to a White House priority, DOJ, DHS, and the ODNI joined with state, local, and tribal partners on a major new endeavor—the SBU/CUI Interoperability Initiative.

□ This effort is developing strategy, architecture, implementation plans, and security and privacy guidelines to establish and maintain a federated, interoperable environment of multiple SBU/CUI networks.
Reinventing Public Safety Model
Information-Led Productivity Gains

The power of information gathered through interagency collaboration cannot be understated in its ability to accelerate results and produce efficiencies across domains.

- Fusion Centers
- HIDTA
- JTTFs
- DEA Task Force Program
- Nationwide SAR Initiative
While there are numerous advocacy groups for public safety organizations, there is no single clearinghouse for coordination of efforts between these often disparate bodies. (such as CJIS, APB, CICC, Global, Nlets, IACP, and NAPO)

State and local agencies are eager to develop awareness of emerging information sharing options available to them...Thus the leadership of public safety organizations and advocacy groups must own and lead the community and its partners in this important endeavor (emphasis added).
Reinventing Public Safety Model
Defining the Way Forward

- Developing the way forward ... must be owned and driven by the public safety community itself, with the strong support of other stakeholders.

- The leaders ... must be mindful that a distributed, decentralized system that builds upon existing technologies is necessary to yield an effective solution, rather than expecting a centralized top-down approach.

- While the ISE is guided from the federal level ... the federal response in this case should be centered on empowering and enabling the law enforcement community to define its own future.
Reinventing Public Safety Model
Defining the Way Forward

The following are first steps to initiate the process of determining the appropriate strategic direction:

- Establish a body of senior Public Safety representatives to create baseline needs and requirements.
- Through a survey of members, identify existing technologies and solutions that can be leveraged by the community.
- Link requirements and needs to Federal funding sources delivering the greatest benefit to the Public Safety community.
Reinventing Public Safety Model
Defining the Way Forward

- Identify cross-cutting capabilities with common attributes, such as RMS and CAD, and deliver a proposal to industry to provide these standards-based services on a pay as you go model, potentially in the cloud environment.

- Leverage common standards framework to assure the delivery of interoperable and relevant products from industry, lessening integration and upgrade cost.
Reinventing Public Safety Model
Defining the Way Forward

- Align and coordinate efforts with other FSLT, CIKR and private entities and programs to accelerate delivery and access to shared services that improve information sharing and operations.

- Develop an overarching strategy map emphasizing the direction and priorities of the community.
What is Federated Identity Management?

**FUNCTIONALLY:**

- You depend on another organization to identify their users and authenticate them before they can connect to your System. A Trusted Identity Provider (IDP).

- Your System relies on the Identity Information provided from the IDP to make access and authorization decisions. (relying Service Provider) (SP)

- IDP’s and SP’s have mutual technical and policy obligations to meet for participation in the Federation.
Global GFIPM Resources

- GFIPM Federation Organization Guidelines
- GFIPM Operational Policies and Procedures Guidelines
- GFIPM Implementation Guide
- http://it.ojp.gov/gfipm
What’s in the GFIPM-Metadata?
(Attributes supporting Role Based Access)

- **User Identification**
  - Info about a person who has an identity in the federation

- **User Certifications and Memberships**
  - Can help an SP make access control decisions

- **User Contact Information**
  - Contact info for the user, his/her supervisor, employer, etc.

- **User Organizational Affiliations**
  - Info about the user’s employment status, assignments, etc.

- **Authorization Context**
  - Supplemental info to help a SP make access control decisions

- **Electronic Identity**
  - Info about the user’s electronic identity (type, issue date, etc.)

- **Authentication Context**
  - Incorporates SAML 2.0 authentication context
What is Global Federated ID & Privilege Management? (GFIPM)

- An authorized set of Trusted Identity Providers (IDPs)
  - Provides Identity information via a NIEM Justice Credential to Service Providers (SPs)
  - Performs local authentication of users and services.

- An authorized set of Service Providers (SPs)
  - Relies on the authenticity of the NIEM Justice Credential Identity Information (relying Service Provider (SP)
  - Makes access and authorization decisions based on NIEM Credential identity attributes.

- IDP’s and SP’s have mutual technical and policy obligations as specified in the GFIPM Governance Policy documentation
NIEF/GFIPM Federation

Single Sign-On (SSO) Solution

Secured Internet
(SSL/TLS (https))

CISAnet

CJJIS FBI
Trusted Broker

LA COUNTY
CCHRS

STATE & LOCAL
Fusion Centers

RISS

HSIN & HSIN (Intel)
Dept. of Homeland Security
CJIS FBI Trusted Broker/Portal

- Trusted Identity Broker Services (Security Token Services (STS))
- IDP Software Services offered to LEA Agencies
- Support for Multiple ID Credential Types
  - GFIPM SAML 2.0 Credentials
  - Direct Access with RSA Advanced Authentication
  - CAC/PIV/PIV(I) Card Access
Issues related to Federated Identity

- Cultural Change to how we do business

- Need to maintain system integrity, such as through audit, training, user management, security

- No longer fits CJIS “CSO Model” for doing that
Issues related to Federated Identity

- Brings in new systems and partners not familiar with CSO Model
  - May not vet users in same manner
  - Audit policies may be different
  - May have different use and dissemination rules
Issues related to Federated Identity

- In the CJIS environment, creates ability to quickly add many users of CJIS Systems from within a state without state’s CSO direct involvement.

- Creates same ability to add many users to other systems which adds to their respective training, auditing, security and other governance requirements.
Issues related to Federated Identity

National Information Exchange Federation (NIEF) Created in 2008 by:

- Criminal Information Sharing Alliance (CISA)
- Pennsylvania Justice Network (JNET)
- Regional Information Sharing Systems (RISS)
- U.S. Department of Homeland Security (DHS)
- Los Angeles County
- Federal Bureau of Investigation (FBI)
Issues related to Federated Identity

Is clearly moving forward from within CJIS for CJIS Systems and within the national environment

- “Direct Connect Task Force” under the CJIS APB process is looking at how to make it work
Discussion Points for Federated Identity

- Are you moving forward with Federated Identity in some form in your state?
- Where do you see liabilities? Benefits?
- What issues do you see for your systems/agencies?
- What questions do you need answered?
- Where do you see costs?
- Who should be the policy leaders?
- Is Federated Identity receiving adequate national policy discussion.