

The IACP Information Integration Planning Model

By Albert Arena, Coordinator, Criminal Justice Information Sharing Project, Research Center, International Association of Chiefs of Police, Alexandria, Virginia

During the height of the Washington, D.C.-area sniper investigation in October 2002, investigators received a reported 142,000 calls from the public with tips and leads. For years the FBI's Rapid Start System has been used successfully in investigations, but the system was not designed to handle multiple shootings crossing several jurisdictions.

To overcome this difficulty, officials adopted a patchwork approach, sorting through piles of handwritten notes and redundant investigations, manually entering information into databases, searching for data in different systems. Although the eventual capture of the accused snipers at a roadside rest stop in Maryland brought to an end a three-week reign of terror, the need for an integrated information system was highlighted during this investigation.

11-Step Plan

Enhanced justice information integration and sharing is essential to improving the quality and effectiveness of law enforcement. Building the infrastructure and systems that allow access to information for law enforcement, prosecution, court, and corrections officials enables informed decision

when timely access to useful data is available. Each of these diverse processes together can make or break a department or agency. The IACP had all of these activities in mind when it developed an 11-step information integration planning model, available online at www.theiacp.org/documents/pdfs/Publications/cjinfosharing.pdf. This plan reflects the expertise and experience of justice and information system experts in five states. The model provides a logical framework within which any jurisdiction can work to improve integration and sharing of data.

Step 1--Bringing Key Stakeholders Together: Key stakeholders are persons who will establish the governance structure and decision-making process. They represent the agencies and organizations that have a vested interest in sharing information and building a foundation for support and funding, and they include police and fire officials, members of city and tribal councils, judges and prosecutors, and others.

Step 2--Developing a Governance Structure: Establishing a governance structure ensures effective planning and decision making. It should contain a mix of people with different talents and skills and well-defined roles and responsibilities. The committee structure lends itself to providing the leadership and technical expertise necessary for managing large-scale technology projects and reassuring community leaders and elected officials that their system will provide

important services and safeguards against privacy violations.

Step 3--Developing the Decision-Making Process: Usually built into the governance structure is the decision-making mechanism that specifies how decisions are made, who makes them, under what authority, and who carries them out. For instance, in the governance structure of San Diego's Automated Regional Justice Information System (ARJIS), depicted in figure 1, the board of directors, which comprises mayors and city council members from participating jurisdictions, has executive powers—that is, it approves the ARJIS budget, makes decisions, and has ultimate accountability for the system. The board makes its decisions under the authority of a joint powers agreement and bylaws agreed upon by all participating jurisdictions.

In the governance structure of some information sharing systems that serve just one jurisdiction, the ultimate decision-making authority and accountability belongs to the police chief or sheriff, who is typically supported by a steering committee composed of deputy chiefs or sheriffs. That steering committee oversees a project manager who directs the work of teams of technical experts and system users (e.g., patrol officers and dispatchers).

Successful integration projects require frequent meetings and updates in order to gain and maintain support. A technique for keeping the stakeholders informed is to post minutes of

meetings and other notes by e-mail or on a Web site available to all stakeholders. Some projects even have a Web site for communicating this information to team members.

Step 4--Developing Goals: An important function of the governing board (or chief executive) is to develop the goals of the criminal justice information sharing system. The place to begin is with a mission statement that will then drive the philosophy and serve as the foundation for the goals that will govern development of the system. Goals should be realistic and achievable, with tasks and milestones in place to measure progress.

Step 5--Determining the Project's Scope: Here the governing board determines what will be included in the criminal justice information sharing system. The board determines which agencies will share, who should have access, and how to deal with security and privacy issues.

Step 6--Completing the Needs Assessment: During this step, an inventory is made of existing system capabilities. In addition, applications hardware and software resources are inventoried, and participants identify critical information exchange points for systems that share data.

Step 7--Creating the Information System: With steps 1-6 completed, the project can next move to the system design and development phase. In this phase, the governing board should hire a project manager to direct all activities related to planning and implementing the criminal justice information sharing system such as selecting hardware and software, building databases, and creating links with federal, state, tribal, county,

and municipal agencies and departments.

Step 8--Assessing Costs and Securing Funding: This is the tough part, requiring the governing board to develop a realistic and comprehensive cost estimate for the new system and then find the resources to fund the project. The board should divide the costs into three categories: planning costs, design costs, and development costs. This division makes it easier to predict how much money it will take to build and maintain the system. The governing board should remember to keep key budgetary decision makers in the loop and actively involved in the funding process. Funding can come from federal grants, bond issues, user fees, and other creative financing mechanisms.

Step 9--Implementing the System: The criminal justice information sharing system is now ready for operation. By now the system will have been tested and debugged by users, technicians, and managers. During the early implementation phases it may be necessary to allow parallel processing of the old and new systems in order to help agencies involved make a smooth transition and to ensure reliability and validity of the data. After a predetermined period for the transition has elapsed, the old system should be shut down and the new one should become fully operational.

The authors of the IACP Information Integration Planning Model recommend that the following activities be undertaken by the state, local, or tribal jurisdiction taking delivery of the system for a successful implementation: develop a strategic plan, train users, create a help desk,

transition in phases, and encourage feedback. These activities inspire confidence among users, ensure quality of data input, and make accountability a watchword for management.

Step 10--Informing and Educating the Community: This step focuses on two communities: the law enforcement community and the citizens. To keep the law enforcement community informed and educated, the system's governing board and managers should hold regular meetings and briefings and should issue reports frequently to garner support for the project and provide a mechanism for feedback that will help guide system architects in their design and development efforts. Training should be made available at all levels of law enforcement. Regular update reports at various law enforcement conferences and meetings can help keep the criminal justice information system in front of every one.

The media can increase public awareness of the integration. The governing board should designate someone to handle the public affairs function to respond to requests from citizens and the press. Include labor representatives and elected officials in media briefings to generate interest, excitement, and anticipation for the system.

The advantages and disadvantages of media involvement should be considered carefully. Many integration efforts can be learning processes; in some cases, publicity may bring attention to mistakes or give rise to expectations that cannot be met. The governing board should see to it that system participants educate media representatives about the complexities of the

integration process.

Step 11--Evaluating and Maintaining the System: Once the system is operational, the project manager should implement a mechanism for measuring user satisfaction and operational reliability, establish a long-term maintenance plan, and resolve any questions regarding warranties, technical support, consultants, and related issues. Authors of the IACP Information Integration Planning Model recommend not waiting until the last minute to build a maintenance capability. Rather, make it a part of the overall planning process.

Critical Issues

Success in building an information sharing system can be derailed if consideration is not given to the critical issues that influence the planning model. These issues help define the mission, identify requirements, fund the project, and ensure that the network is trusted, dependable, and ubiquitous.

Personnel: Among the necessary personnel is the project manager who oversees daily operations and communicates with executives and others to discuss policy issues as they arise. He or she understands criminal justice processes and systems, is technically proficient, and is good at negotiation and delegation. He or she makes all the pieces fit.

Business Process

Reengineering: This process is an assessment of the day-to-day operations of the criminal justice system. It's the forms, steps, and procedures (including legal) that occur within the system and that are shared with other internal and external agencies and departments.

Results from this process drive software development and help ensure a product that meets the needs of all parties.

Funding Strategies: Funding may present a major challenge to integration and is often a factor in defining the scope of the integration effort. Without funding, the system will never get off the drawing board. System executives should consider appeals to state legislators, county appropriations boards, federal grantees, and local taxing and governing entities to obtain the necessary funding.

In a statewide system it is possible that several independent integration efforts may occur at one time. Part of the planning process includes doing an intake of ongoing integration efforts to ensure all components will be interoperable and funding is available to coordinate and integrate the various systems into one criminal justice information system.

System Architecture: Sharing information is much easier when systems are open and interoperable. The project manager should make technical specifications readily available to software developers, should consider scalability, and should enforce standards. The Office of Justice Programs' information technology Web site (<http://it.ojp.gov/index.jsp>) maintains the latest information related to standards, and its practical applications for improving criminal justice strategic and tactical operations.

Vendors: Most likely there will be several vendors working to implement any new system. Consultants, database managers, software and hardware developers, and outsourcing firms will probably all be

needed for the integration effort. Selecting vendors carefully will save time and money over the life cycle of the project.

Privacy and Security

Requirements: At a minimum, the information sharing system should conform to title 28, part 23 of the Code of Federal Regulations throughout the collection, access, storage, and dissemination process of criminal intelligence data, whether or not the system is federally funded. Compliance will help protect the privacy and constitutional rights of persons and groups. Keeping a system free from hackers and invulnerable to both natural and manmade disasters requires planning and preparation. Some basic defenses include firewalls, user background investigations, passwords, and virtual private networks.

Data Integrity: Ownership, standards, and definitions make up what is necessary to ensure data integrity. End users and technicians should resolve these issues before implementation the help ensure that the system will perform reliably and in the best interests of the public.

Build It, and They Will Use It

Taking these 11 steps and paying attention to the attendant critical issues should help create a solid foundation for a criminal justice information sharing system that satisfies the demands of practitioners and the public.

For more information regarding the planning model or criminal justice information sharing, call Albert Arena, project coordinator, at 800-843-4227, or send an e-mail message to him at arena@theiacp.org.