three: enterprise system implementation

Policing Smarter Through IT: Lessons in Enterprise Implementation

III. Enterprise System Implementation

Operational level

The CPD's experience revealed five facets of implementation at the operational level that had a significant impact on successful application deployment: conducting a physical capacity assessment, generating internal marketing, capturing officer feedback, providing officer training, and establishing a user support process.

Physical capacity assessment

The untimely realization that the physical facilities available in the field cannot accommodate a new IT application can be a critical roadblock to a successful application launch. Once an application's development plan is in place, it is important to conduct an assessment of the physical capacity of stationhouse facilities' hardware, software, lighting, wiring and other infrastructure elements to make sure that all of the pieces are in place for a successful application roll-out.

In the CPD, for example, this was carried out by officers who went to each of the department's stationhouses to examine their capacity to accommodate the enterprise system. They assessed existing hardware and the physical capacity of the stations to accommodate the users who would need to access the system. The assessment consisted of room-by-room examinations (front desk area, sergeants' offices, interview rooms, tactical office, lockup, radio room, etc.) of available space, existing computer hardware and operating system configurations, the availability of Internet connectivity ports, and even the station's power supply and wiring. Rarely are stationhouses

prepared for a major new application. While the following recommendations are generally applicable, they are by no means a guarantee of implementation success, and members of the development team with a good understanding of system and user needs must be involved in capacity assessment in a hands-on fashion.

Assessment team: It is vital that the team or individual selected to conduct assessments have, in addition to ample policing experience, a wide array of skills, including knowledge of hardware and current technology trends; an understanding of the application's hardware requirements and impact on space utilization; and a basic knowledge of electrical wiring. It is important for the assessment team to be aware of the organization's plans, such as when stationhouses are scheduled to be renovated or replaced, as well as the effect that these plans will have on an application's launch. The assessment team must also be able to discern between a facility's true equipment needs and officers' well-meaning attempts to fill their wish lists.

Safety: When performing facilities assessments, officer safety must be kept at the forefront. Astute assessment teams will recognize potential safety and operational advantages of certain types of hardware. For example, flat-panel computer screens may be preferable to traditional monitors because they take up less space and provide a less-obstructed view of offenders during arrest processing. Power outlet location also requires careful consideration to reduce safety concerns – especially in arrest processing rooms. Outlets located too far from workstations or too close to prisoners could place lengthy power cords within prisoners' reach, leading to processing disruptions, injury to prisoners or officers, or equipment damage. Also of concern in the arrest processing room is furniture installation: computers must be bolted to desks that are secured to the floor. Care must be taken when considering furniture options, as not all tables and computers can be easily anchored together.

Application design requirements: Another key element of a facilities assessment is a thorough understanding of extenuating circumstances that impact application utilization. For example, in the CPD, juvenile arrests must be

processed in a separate room using a computer dedicated to juvenile-offender processing. In contrast, arrest processing of adults can take place in numerous processing rooms with shared computer stations. Hence assessments must determine the number of computers needed for stand-alone tasks, as well as a count of those to be used for shared officer tasks. Providing sufficient and strategically placed computing resources can reduce user dissatisfaction with new applications.

A facet of the CPD's automated case reporting system further highlights the need to consider every possible impact that an application may have. In the near future, officers will be able to wirelessly complete and submit reports using data terminals mounted in their cars. This advance makes the availability of spare fully charged portable data terminal (PDT) batteries very important. Aware of this, the assessment team needed to determine the minimum number of PDT batteries and chargers to accommodate each district's personnel roster, as well as the optimal type of battery to be used in Chicago's frigid winter climate. Climate also affected the choice of computers, for flat-screen LCDs have a habit of cracking when the temperature in the car drops too low.

Anticipate issues: A good physical capacity assessment should anticipate potential problems when a complex computerized system is deployed. These can be basic environmental issues as well as technology-related obstacles. One such unexpected environmental problem – dim ambient lighting combined with dingy walls – limited the initial effectiveness of the CPD's new mugshot system at several sites. In the technology category, outdated PC operating systems, which are easy to overlook because they are, by nature, operating in the background, caused aspects of newly developed applications to malfunction.

In addition, ensuring that virus protection software is up-to-date on each workstation is critical. System functionality can be brought to a halt by an undetected virus.

Internal marketing

RANK-AND-FILE RESISTANCE TO NEW APPLICATIONS CAN BE DIMINISHED BY A WELL-CONCEIVED MARKETING CAMPAIGN.

Another important facet of implementation at the operational level is the use of internal marketing to generate early excitement about an IT application. Rank-and-file resistance to new applications can be diminished by a well-conceived marketing campaign. In the past, newly introduced automated systems sometimes met significant resistance in the CPD, especially among veteran officers with limited computer experience. The department's current approach is to raise awareness of applications under development well in advance of implementation. Early internal publicity can highlight the project's benefits for the average officer.

Marketing efforts should try to derail predictable complaints such as, "It'll take me longer to fill out a report online." and focus on the advantages offered to users by the new system, such as the increased availability of accurate data and increased report legibility, the ease of making corrections, the convenience of drop-down menus, the ability to copy information from form to form, and the like. Care must be taken, however, not to "oversell" the new application and foster unrealistic expectations. Marketing campaigns can consist of memos and promotional literature or videos, coupled with articles and information posted on law enforcement web sites to help generate interest and a sense of pride in being a leading-edge department. Kickoff meetings provide an opportunity to create excitement among those closest to the application, with the possibility of trickle-down effects to other parts of the department. If nothing more, these measures may stimulate officer dialogue about a new application, making them feel a part of what is happening and better prepared for changes in their day-to-day tasks.

Testing and feedback

> *... IT IS IMPORTANT TO CREATE AN AVENUE FOR OFFICERS TO PROVIDE ONGOING FEEDBACK.*

Garnering feedback from future users is an ongoing process in the CPD. It routinely begins in the conceptual design stage, continues during developmental brainstorming sessions with potential users, and takes on increasing significance during often extended implementation periods. As late as the pre-launch phase, groups of officers can provide feedback on test versions of an application, and pilot test it in the field. Officers have an incentive to provide critical feedback, knowing that they will soon be routinely using the application. Most officers appear eager to provide open and honest feedback about an application's strengths and weaknesses.

Our observations in the CPD yielded a few key factors related to testing and feedback. First, care must be taken to select skilled, conscientious, and open-minded officers and allow them adequate time to thoroughly investigate and evaluate all of an application's functions. The more time spent evaluating, the more likely it is that flaws will be found and corrected before implementation. While it may seem unnecessary to point out that follow-through is important when eliciting feedback, we observed that for one of the CPD's applications, officers were encouraged to fill out feedback forms that were never collected.

It is recommended that a team of testing officers be assembled over a predetermined period of time (days, weeks or months, depending on the complexity of the application) and be given the opportunity to focus solely on testing the application. If this is not feasible, general feedback from users in the field can be fruitful, but it is apt to be less

systematic. Testers who are asked to test an application during their downtime – rather than in a formal testing setting – are not apt to provide in-depth feedback. It may be necessary to hold roll call reaction sessions or other types of gatherings to elicit meaningful recommendations. Finally, after full implementation, it is likely that minor bugs and glitches will surface. Therefore, it is important to create an avenue for officers to provide ongoing feedback. An effective option is to provide an e-mail link for reporting errors so that officer feedback can be sent directly to those in charge of maintaining the application.

Training

Successful implementation is dependent on adequate user training. The CPD has several training options, all with varying degrees of cost, time, and effectiveness.

Roll call training: A basic form of user preparation is roll call training, which relies on streaming videos displayed in the roll call room, departmental memos, handouts, or presentations by trainers. Because roll call can bring officers and civilian personnel together in the presence of a supervisor, it is a cost-effective method for delivering instruction on less-complex applications, and it is especially effective for introducing upgrades to existing systems. We found this training delivery method to be most effective when a trainer was on hand during the presentation to answer questions about the new application and remained available for a period of time afterward to provide hands-on assistance as needed. However, from our observations, unstructured roll call training often falls on the ears of disinterested and unresponsive officers.

Classroom sessions: Training users on more complicated applications usually requires hands-on instruction at an appropriately equipped site, with skilled trainers delivering a customized curriculum. For example, the automation of

the entire arrest process in the CPD requires one full day of training for every police officer, and an additional day of training for all supervisors and managers. Training on this scale is a costly venture and, in a big city agency, a logistical feat; nonetheless, this configuration can be essential for complicated systems that are vital to the organization's operation. It is also important to have several trainers available in the classroom to provide individualized over-the-shoulder attention to participants, as needed, to allow the primary instructor to keep the lesson moving along.

On-the-job training: On-the-job training can be used to familiarize officers with new applications in their work environment at the time of implementation. It requires a carefully assembled team, often consisting of one or two trainers and a technical expert to handle troubleshooting. This method generally captures officers' attention because of the individualized attention and immediacy of the setting. In the CPD, for example, it was possible for training teams to personally instruct lockup keepers in the use of a new digital mugshot system as they continued to process arrestees. Care should be taken to ensure that all "day-off" groups are accommodated. District personnel on each of the three shifts should be identified to provide later instruction to those who were not present for instruction delivered by the trainers.

Train the trainers: In this instructional option, designated officers are trained in a classroom setting and, once familiar with the application, are sent back to their respective units to train fellow users. The CPD, for example, trained designated representatives from suburban Chicago police agencies on the use of the data warehouse in a half-day classroom session at police headquarters. Approximately 20 participants attended each session. Those participants, usually two per agency, in turn trained others in their respective police departments. While this is a cost-effective method, it is difficult to maintain quality control of the curriculum and its delivery.

Supplemental training material (user manuals or bulleted tip lists) effectively augment training of all kinds. Lists of problems and solutions or answers to frequently asked questions are useful because they can be posted in officer workspaces to provide a quick reference. Training manuals that detail instructional sessions or more general user manuals can function as comprehensive reference tools. In the CPD, officers with limited computer experience seem to prefer having printed user manuals to remind them how to use aspects of the application, as opposed to more seasoned users who are comfortable with online help options, tip lists, and online supplemental materials.

> ...KNOWING WHO HAS BEEN TRAINED IS KEY.

An important training component is tracking; knowing who has been trained is key. Without an accounting system in place it is nearly impossible to know whether all users have undergone training and difficult to determine how long to continue offering training sessions, as well as whom to target. Accurate recordkeeping can prevent situations in which users claim that they do not know how to use an application because they were unaware of training sessions.

Finally, it is advisable to think through a new application's dependencies on other applications and whether users are adept at using them. If the other systems are complicated by or changed in conjunction with a new application's launch, it may be necessary to include instruction on how to use them as a part of training for the new application.

Multi-tiered help system

Successful implementation of any IT application calls for a multi-tiered help system, allowing users to quickly access accurate information.

Self-help resources: One line of support is help functionality built directly into an application so that with a few clicks of the mouse, officers can find answers to their questions. Another self-help option is the use of reference tools – training booklets, user manuals (printed or online), and a printed troubleshooting list. Self-help resources are especially advantageous for personnel who may be covering for a co-worker with different day-to-day duties.

> A RELIABLE SYSTEM FOR CALL-BACKS MUST BE ESTABLISHED...

Go-to person: In some cases, self-help resources will not be adequate, and it is advisable to appoint several liaisons or "go-to" persons at each facility who can clear up confusion and provide user support. The advantage of having such a designee is that officers often feel more secure about using new applications when a knowledgeable co-worker is available to answer questions and help them troubleshoot problems. However, identifying a willing "go-to" person available on each shift may be difficult, as this is usually an added responsibility for an already-hardworking person. At times, this person will be unavailable to respond to user issues in a timely manner. Another pitfall of relying on a go-to person as a primary resource is that personnel transfers, medical leave, or retirement can leave a unit unsupported.

Help desk: A thoroughly trained and well-managed help desk is a valuable asset to users. The help desk is a key contact point, for callers expect resolution of their problems when they make the call. Without a reliable help desk, users can overlook vital features and lose the benefits of new applications. A help desk can be a vital support system in organizations such as law enforcement agencies, which operate around the clock.

Help desks have great potential for enriching the user experience. However, if the help desk is not well managed or adequately trained, breakdowns in procedure and performance are likely. As in any customer-client service situation, callers expect a prompt, knowledgeable response. A coordination challenge unique to law enforcement agencies is related directly to the nature of officers' jobs. Because officers spend much of their time in the field, it can be difficult for help desk personnel to reach those who require return telephone calls to resolve issues. A reliable system for call-backs must be established or the help desk system will not be an effective resource.

THE IMPORTANCE OF CONDUCTING A THOROUGH AND DETAILED PROCESS-MAPPING OF THE ORGANIZATION CANNOT BE UNDERSTATED.

Over-reliance on developers or vendors is another pitfall in operating a help desk. When a new application is launched, it is likely that help desk staffers will not have sufficient experience to troubleshoot all problems. As a result, it is likely that the help desk will rely heavily on developers and vendors for higher-level problem resolution. It is vital that comprehensive training be offered to help desk personnel so that the need for external support is diminished. That said, as the number of applications introduced in an organization increases, help desk representatives may find it difficult to maintain a high level of familiarity with each computer program. To keep the help desk functioning at a high level, it is advisable to create a searchable knowledge database – a compendium of solutions that have been reached for previous queries.

Good internal communication is also important for help desk effectiveness. Help desk personnel should be among the first to know when system maintenance is scheduled, when systems go down, and when new applications are to be launched. Help desk administrators should be aware of application deployment schedules so that they can

provide adequate personnel to meet anticipated increases in calls. Tallies should also be kept on recurrent questions, because later analysis may reveal needed changes to programs or new areas of emphasis in training.

Organizational level

Based on our observations in the CPD, four organizational-level issues deserve mention as considerations when developing an enterprise system in a law enforcement environment: scheduling, privacy and security mechanisms, external data sharing arrangements, and diversionary pressures.

We have seen countless unexpected events undercut carefully crafted schedules and impact timely IT implementation. We learned that internal unit coordination is essential, that buy-in is much greater with the inclusion of stakeholders in the planning process, and that unanticipated personnel changes can dramatically alter implementation schedules. Adequate privacy and security mechanisms need to be in place, external data sharing arrangements require in-depth consideration, and lastly, diversionary pressures always emerge when they are least expected. The following section discusses these organizational-level implementation issues.

Setting schedules

When developing a large IT project in a complex environment, developers usually start working on many application modules that will eventually be merged into a complementary system. Because these applications are often dependent on one another, roadblocks in one can create a chain reaction that stalls advances on many other applications. These hold-ups can appear to be terribly large and troublesome and are often linked to some overlooked step during the development phase. Creating or fixing some of these steps can be costly, complicated, and time consuming. Anticipating the unexpected is difficult. Predicting launch dates for applications with

interdependencies is difficult. The importance of conducting a thorough and detailed process-mapping of the organization cannot be understated. Each unit, person, and function should be accounted for during the process-mapping task. By looking at department needs, gaps, and overlaps, potential problems can be identified and addressed before the implementation stage.

Setting schedules for implementation must also take into account personnel changes that may take place within the organization. Large police departments make personnel changes often and with little notice. Officers working on IT projects hope to be promoted, and this usually leads to new assignments. Others will retire, often with little advance notice. This environment can hamper the successful implementation of an IT project. A single person should not be expected to carry out the critical tasks of project implementation. Relying on people who may be put back on the street or promoted can spell disaster for such endeavors. While input from officers is important and necessary, it is a good idea to have project managers that do not disappear in the night. Finding people in the organization who can sustain their positions throughout the length of the implementation phase is critical to adhering to project schedules.

Developing security and privacy policies

Criminal justice agencies developing an IT system are responsible for anticipating privacy and security issues at many levels. While data sharing holds tremendous promise in terms of problem-solving, predictive analysis and cost-effectiveness, inherent in it is the ongoing threat of revealing data inappropriately or violating citizens' rights. Prior to implementation, policies will need to be developed to balance officers' need for information with the risk of data misuse. At every level, policies must be in place that determine who should have what information and under what circumstances.

Increased information, used properly, can translate into increased case clearances and, even better, increased crime prevention. (This assumes that the police department is properly deploying officers and communicating with residents at a rather sophisticated level.) However, when communicating with residents, there are important factors that go into deciding what information is useful to them and what information may be violating others' rights to privacy. Security and privacy policies need to be created for internal use, as do policies that determine what data can be safely shared outside the department. Each unit and rank should have access to information at levels pre-determined by their supervisors.

INCREASED INFORMATION, USED PROPERLY, CAN TRANSLATE INTO INCREASED CASE CLEARANCES AND, EVEN BETTER, INCREASED CRIME PREVENTION.

Additionally, accountability systems must be created to ensure security of the data. A system that monitors and regularly checks data usage is critical to maintaining the integrity of the information in the system. Policies must be set concerning the level of access available to personnel at various ranks, and under what circumstances management and personnel data can be accessed. It is very important to identify the circumstances under which existing crime and arrest records can be modified, a vital point for maintaining organizational integrity.

Policies need to be developed for handling cases of data misuse, when it occurs. This means that each system user should have a unique identification number that controls his or her access to information. This way each data query can be linked back to the person conducting the search. Only when individual officers know that they will be held accountable for their behavior can an organization have confidence that the majority will properly utilize the information. The system should be able to detect any unusual activity.

We observed one example of this which involved an officer who was questioned about why he was making so many queries to the system. While this activity was not inherently wrong, it was unusual. In this case, the officer was conducting queries for many other officers because they did not know how or want to use the system. While this did not point to data misuse, it did uncover the need for more work in addressing officers' resistance to using the technology or the need for retraining.

WITH THE NEED FOR INCREASED SECURITY FROM OUTSIDE THREATS HAS COME THE PARALLEL NEED FOR SHARING INFORMATION WITH OTHER AGENCIES.

Finally, criminal justice agencies are frequently called upon to expunge data. Making data "disappear" is not the instinct of database developers, but it may be a legal requirement that protects the rights of juveniles, people who are found innocent, or citizens who have been the target of police investigations. Data that is held in one place is easier to expunge than data that spreads ("propagates") itself around to many discrete corners of the organization. This should be taken into account in database planning. The question of whether backup and archived data should be expunged is a thorny one, but one that also must be considered.

External data sharing

Most police departments have tightened their security practices in response to the threat of terrorism. With the need for increased security from outside threats has come the parallel need for sharing information with other agencies. The more information available to an agency, the better equipped it is to deal with emergency situations. In addition, the usual routines of police work are more effective when a wide network of information is available because, like terrorists, everyday criminals pay no attention to municipal boundaries.

By implementing the CLEAR system, the CPD has taken the lead in a large-scale criminal justice, web-based information-sharing project that involves several hundred law enforcement agencies, prosecutors, and federal agencies. They have access to a growing body of crime, arrest, and investigative data that is being centralized in the CPD's computers. Several key issues that emerged as this criminal justice integration project developed were noted in the evaluation.

It turns out that building a solid enterprise system to support a cooperative network of information sharing is not enough to make it happen. The system must be marketed to potential users in a manner that demonstrates both the benefits to other agencies and the ease of using the system. This requires knowing users' needs, aggressively pursuing potential users, and providing start-up and ongoing help to keep things moving.

For example, a retired police lieutenant holding a civilian position within the CPD serves as a full-time "salesperson" for the system. He approaches agencies in surrounding communities to explain and demonstrate the system, and follows up on all inquires by other agencies. A fair amount of technical hand-holding is provided for those who need it. Participating agencies can send officers to the CPD for specialized training at no cost. While this is a task-intensive outreach effort, having data collected by and accessible to surrounding communities has had a profound impact on clearance rates and has led to the development of new partnerships among those agencies and the CPD.

For other jurisdictions, getting information from the CPD has become just a "click on the keyboard," as opposed to the past effort and expense involved in sending someone downtown to wait in line for 'this' or 'that' file folder. Neighboring agencies are solving serious crimes in a much shorter time period using information from the CPD's data warehouse. Feedback to-date supports the value of the external data sharing endeavor, despite its implementation challenges.

To make an integrated data sharing project work, the enterprise system behind it must be easy to access by other agencies, yet also be secure from inappropriate use. Experience has documented the critical importance of knowing who is accessing what data, where, and when. Every user has a unique identification number that must be used for each and every data query. System training stresses the importance of reporting any potential misuse of the data warehouse information. In one instance, a cooperating department found a CPD data warehouse printout in the home of an offender. User accountability procedures built into the system enabled the CPD to identify the officer who had printed out the report, and the matter has been investigated. While such incidents are optimally infrequent, the importance of having a system in place to detect such behavior cannot be understated. Any department that holds important and personal information must be able to ensure that it will be used appropriately, and that those who misuse the information will face serious consequences.

EXPERIENCE HAS DOCUMENTED THE CRITICAL IMPORTANCE OF KNOWING WHO IS ACCESSING WHAT DATA, WHERE, AND WHEN.

Adapting to diversionary pressures

One of the big challenges police departments face when initiating any new IT development project is being able to keep officers and resources slated for the project in place for the duration. This is difficult because policing is so inherently reactive to events outside its control, and also because the public has little interest in the improvement of back office operations if it appears to come at the expense of responding to emergencies. As a result, over time, the CPD has taken on strategic initiatives that are in some ways at cross-purposes with IT development. Like any

metropolitan department faced with the formidable task of addressing high crime rates, the CPD has had to redeploy to on-the-street assignments officers who are key players in the development of IT projects.

ANY POLICE DEPARTMENT PLANNING AN IT SYSTEM NEEDS TO CONSIDER THE REACTIVE NATURE OF THE DEPARTMENT'S WORKLOAD...

Training is a labor-intensive part of a major IT initiative, but in a busy department relatively few officers can stand down from duty at a particular time. When officers' and supervisors' work assignments are in flux, carefully crafted planning and training schedules can come undone overnight. This also applies to deadline-bound application developers who are called on to regroup and address more immediate and pressing problems facing the department. These situations will present problems in smaller departments as well, since they have fewer people to redeploy. Any police department planning an IT system needs to consider the reactive nature of the department's workload and schedule flexibility into the project implementation phase to accommodate both internal and external diversionary pressures.

four: assessment

Policing Smarter Through IT: Lessons in Enterprise Implementation

IV. Assessment

> *New projects and new expectations must be backed up by supervisors...*

Organizational assessment

Serious self-assessment is not easy in any organization, yet it is a critical step to knowing whether an initiative is making a difference in operations or helping an organization meet its goals. A new IT project may look impressive, but knowing whether a department functions any better as a result requires deeper analysis. There may have been a consensus that the old system was not working and great effort put into devising a new one, but the final step of gauging the effectiveness of the solution needs to be taken as well. Oftentimes the emphasis seems to be on doing the work, but not on measuring whether the work has made a difference in department goals and objectives. IT projects often begin with lofty goals, promising efficiency, speed, increasing accountability, and the reduction of crime. Only a detailed self-appraisal will uncover whether these goals have been achieved.

Officer assessment

Equally important in the implementation of an IT project is the creation of an accountability structure that matches officer performance measures with new job expectations related to the technology. This is true for any new project. Officers have seen many projects come and go, and are often hesitant to do their work differently simply because new technology has appeared in their stationhouses and patrol cars. Even with training, officers who are not accustomed to using technology may quickly revert back to old ways of doing things or become dependent on a co-worker viewed as the stationhouse "computer whiz" to conduct their queries.

New projects and new expectations must be backed up by supervisors who have an expectation that officers will be working in non-traditional ways. These new expectations should take the form of new performance measures that supervisors take seriously and utilize when making recommendations for officer salary increases and promotion. The impetus should come from the chief's office in the form of orders or directives underscoring the importance of the new project. Officers should know that the department is serious about the project and that it will be measuring appropriate skills and behaviors to ensure project success.

five: conclusion

Policing Smarter Through IT: Lessons in Enterprise Implementation

V. Conclusion

The adoption of information technology at the enterprise level is a strategic decision that does not take place in a vacuum. The CPD's IT plan reflects its problem-solving orientation, which stresses "intelligence-driven" policing, and an internal accountability process that "manages for results." Crime analysis is a line function, not a staff function, for rapid deployment and relentless real-time assessment requires nimble technology and up-to-date data in the hands of those who are actually doing the work.

...RAPID DEPLOYMENT AND RELENTLESS REAL-TIME ASSESSMENT REQUIRES NIMBLE TECHNOLOGY AND UP-TO-DATE DATA IN THE HANDS OF THOSE WHO ARE ACTUALLY DOING THE WORK.

The CPD's commitment to metropolitan (and now statewide) data integration reflects the new reality of American cities: close-in suburbs are facing serious crime problems, drug markets span the metropolitan area, and the spread of gangs is closely associated with both. The CPD's plan to involve community members, and the extensive network of community activists that has built up over the past decade, reflects its commitment to two-way information sharing as part of its community policing program. New information technology thus supports the transformation of the organization and helps it adapt to changes in its environment. Both are good reasons to consider the role that technology can play in helping police meet the challenges of the 21st century.

resources

Policing Smarter Through IT: Lessons in Enterprise Implementation

Resources

All community policing and information technology publications produced by Northwestern University can be viewed at the following web site: **www.northwestern.edu/IPR/publications/policing.html**

Global Justice Information Sharing Initiative. U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov**

Global Justice XML Data Model (Promoting Justice and Public Safety Information Sharing). U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov**

Harris, Kelly J. and Romesburg, William H. Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!), A Guide for Executives, Managers and Technologists, Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, 2002. **www.cops.usdoj.gov**

Information Technology Initiatives (The Information Sharing Resource for the Justice and Public Safety Communities), U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov**
.
Justice Standards Clearinghouse (A Repository for Developing and Established Justice and Public Safety Standards). U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov**

National Criminal Intelligence Sharing Plan. U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov**

SEARCH, The National Consortium for Justice Information and Statistics. **www.search.org**

U.S. Department of Justice, Office of Community Oriented Policing Services. **www.cops.usdoj.gov**

Policing Smarter Through IT: Lessons in Enterprise Implementation

For More Information

U.S. Department of Justice
Office of Community Oriented Policing Services
1100 Vermont Avenue, N.W.
Washington, D.C. 20530

To obtain details on COPS programs, call the COPS Office Response Center at 800.421.6770

Visit COPS Online at www.cops.usdoj.gov

Created: August 31, 2004 **e07042404**
ISBN: 1-932582-83-X