Executive Summary

By Margaret Jacobs

It is remarkable how much benefit a law enforcement agency and consequently the public can experience from a successful mobile computing system. At the very least, the system will store records in a computer that were previously managed by hand. Once computerized, the records can be rapidly searched, easily compiled into reports, and quickly shared with others via electronic transmission. And, with some consideration given to the steps involved in law enforcement processes and the extensive abilities, powers, and capacities that mobile computer technology has to offer, the percentage of savings in time, personnel, money, consumables, accuracy, and safety can be truly monumental, often between 20–40 percent.

Benefits of Mobile Computing

The degree of benefit a department achieves from mobile computing technology depends considerably on which hardware, software, and accompanying technologies are implemented. Yet even with a very basic system, the benefits can be enormous.

Below are brief descriptions of primary benefits generally attained when law enforcement agencies deploy a typical system, which would include mobile communications (with dispatch, the ability to query the National Crime Information Center [NCIC], and local messaging), and field data reporting (incident, accident, and field contact).

Reduced Radio Congestion
The use of computers for queries, dispatch, sending messages, and doing checks cuts down on voice traffic up to 40 percent, opening up voice channels for emergencies.

Lighter Dispatch Workload
Activities such as making status entries on the computer aided dispatch (CAD) system, issuing call assignments via radio, performing NCIC queries and sending the information back to the inquirer can all be done by officers in the field using mobile computing, thereby unburdening the dispatcher of these duties. Cutting down dispatcher workload in this way typically cuts expenses in the dispatch center by approximately $100,000 per year. Floor space and equipment savings can add up to $50,000 per year.

Easier Resource Management, Allocation, and Supervision
Through the use of mobile messaging technology combined with a CAD system, supervisors can know what call their units are assigned to, revise assignments on the fly, and override a dispatch assignment for more efficient use of resources. They can also see in advance when staffing at a scene is likely to be insufficient. Mobile data communications (MDC) technology that allows officers to access police databases may help warn an officer if he has
encountered a potentially dangerous situation. When automated vehicle location (AVL) technology helps pinpoint vehicle locations, it helps the dispatcher or dispatch system direct the closest possible resource to a scene. AVL software can also locate an exact location of a vehicle of a distressed or unresponsive officer, thereby allowing aid to be dispatched to his/her location.

**Cost Savings by Avoiding Paper**
Police work generates reports, which are typically produced on paper. Mobile computing can eliminate using paper for the first round of information collection. Electronic communications can replace paper for information exchange inside the police department. Such paper reduction can produce significant cost savings by eliminating things like copy supplies, copy machines, storage space, and printing costs. It also reduces personnel costs in the areas of making copies and filing, retrieving, and distributing paper records.

**Reduced Data Transformation Time and Improved Record Quality**
In paper-based records collection, officers (who know the most about an incident) capture required data about an incident on paper forms. They then pass those forms to a clerk to be entered into the computer. Clerks must decipher what the officer wrote (causing transcription errors) and resolve ambiguities second hand. And when the clerk enters the record into the computer he/she is capturing that data for a second time, thereby duplicating effort. If the officer enters the report directly into the computer he/she saves the clerks’ office up to $45,000 per year (averaging 20 minutes per report for 10,000 reports per year at $15 per hour). Executives must keep in mind that clerks are still needed; their function shifts to quality assurance, error checking, and data validation. Officer data entry also cuts down on transcription errors and cuts the time it take for data to get into the computer and back out to investigators, thereby increasing the probability that the case will be solved. Higher report quality is also a resulting benefit.

Other benefits include improved intradepartmental communications, support for community-based policing, less expense when a report changes, lower training costs, increased officer confidence, and improved professional image for the department.

One significant operational change derived from mobile computing is that field data entry may drastically reduce the amount of time that officers spend writing reports (thought to be as much as 20 percent of patrol time). Another operational benefit of in-the-field data capture is that officers can reuse data elements for numerous reports, eliminating duplicate data capture on forms. For instance, from one accident an officer may need to generate a DUI report, accident report, and an arrest report. Common information such as driver name and license number can be captured once and used multiple times.
Reworking Business Processes Before Computerization

It is the perfect time, when standing on the threshold of designing a mobile computing solution, before any equipment is chosen, for department personnel to perform a serious review of their business processes.

In the past, during earlier generations of computerization in law enforcement, it was common to simply automate a manual process on the computer. This approach to application development is lacking on several fronts. First, many times it simply computerizes an existing bad process. And, often it does not consider utilizing the power and capacities that computers have beyond humans. Most importantly, it does not link the development of the application to the process it is being built to support. Therefore, it is wise to first redesign processes to make them more effective and productive for field personnel. Then computer applications should be developed to provide improved tools for the field officer, supporting the recently improved business process. In this way users can gain the ultimate value from technology, having the technology enhance the process it supports rather than simply computerizing an existing bad process.

Change Management

For all the benefits a mobile computing system can bring to an agency, it is often met with resistance, especially by older, more experienced officers who feel comfortable with manual processes. Therefore it is vital that they are shown how the new technology will truly make their work easier and safer. Most importantly, they must buy into this idea. Once the officers truly accept the value of this technology, they will make the effort to integrate it into their work habits and eventually will become dependent on it.

When designing and implementing a mobile computing solution, consider first the officers who may have the most difficulty with technology and design your implementation strategy with them in mind. It is wise to include them at the start of the planning phase.

Vital Backup Procedures

Dependence on technology can bring law enforcement work to a grinding halt if the technology fails. Unfortunately, everyone knows that at some point all technology will have downtime. Therefore it is crucial that backup systems are in place, data backups are kept, and spare parts are on hand. Supplies and procedures for manual reporting and radio use should be kept at the ready. Manual procedures should be reviewed and drills on manual processes performed periodically to be sure everyone, especially younger officers who did not initially work with manual processes, can carry on their essential work during technology downtime.

Background of Mobile Computing

When law enforcement personnel think of mobile computing, they may picture the earliest technology solutions from the 1980’s. These consisted of proprietary systems with small screens that were tied to an agency-owned radio system. These were expensive and often
unreliable. In the 1990’s, more sophisticated mobile applications arrived, driven in large part by package delivery businesses (e.g. Fed Ex and UPS). Currently, modern business can pick from a plethora of dependable and affordable options to implement mobile computing solutions for their businesses. The growth rate for this technology is slightly slower in the law enforcement market due to tight budgets, security issues, and complexity of integrating with CAD, records management systems (RMS), and databases. However, it is moving forward at a rapid pace, bringing with it some of the biggest advances in police work in the history of law enforcement.

Some Emerging Technologies

- Currently, there is keen interest in mobile applications that require faster networks that carry larger files, also known as “broadband” applications, which can transmit video, photos (including mug shots) and fingerprints. Law enforcement workers want instant access to complex data from any location.
- In response to 9/11, to acknowledge the need to allocate additional spectrum to support broadband data communications, the FCC designated the 50 MHz spectrum in the 4.9 GHz band entirely for public safety mobile data networks. Existing equipment and industry tested technical standards for broadband transmission speeds work well on this band.
- Hotspots, Wi-Fi, mesh networking (which uses repeaters), multi-path networks (which use multiple networking technologies to achieve best results), and faster networks under development by cellular companies are on the cutting edge of mobile computing.

Technologies Commonly Used Today

For the purposes of this summary, mobile computing is defined as the use of industry standard portable computers in law enforcement patrol vehicles.

There are three types of networks most commonly used for mobile computing in law enforcement today:

- Relatively slow networks that are built, administered, and maintained by the agency itself. This includes regional radio networks that use 800MHz trunked technology.
- Somewhat faster cellular data networks that the cellular carriers operate and maintain (includes a monthly access fee; good for small agency in a region with good coverage).
- Agency installed and maintained Wi-Fi networks that use computer-to-computer or computer-to-base technology. These offer full broadband speed but very limited range.

The three major categories for components that make up the mobile environment include hardware, software, and other associated technologies.
Hardware
Hardware options consist of handheld computers, tablet computers (usually pen-based), and full sized laptop computers with keyboards, which are sometimes pen-enabled. Within the hardware category there are also three other classes to consider – consumer grade laptop computers, rugged laptop computers, and fixed mount vehicular computers.

Consumer grade laptops are the least expensive to buy initially, but the rough patrol car environment causes them to need frequent repairs and have a short life cycle. Also, regular laptop computer screens are difficult to read in bright sunlight, which is often present in the patrol vehicles. While initially two to three times more expensive than a consumer laptop, the rugged laptop has a longer life cycle. It is available with a sunlight readable screen and touch screen option that makes operation much easier in the field. When mounting either of these choices in a vehicle, consideration must be made to avoid interference with air bag deployment. Several vendors also offer computers purposefully designed for use in a vehicle. Screens are readable in direct sunlight, all are touch screen enabled, they are designed for mounting without airbag interference and they cost about the same as rugged laptops.

Software
The two most popular software applications for law enforcement mobile computing are mobile data communications (MDC) and field data reporting. MDC provides immediate access to the information in local, regional, state and federal law enforcement databases. Most commonly officers search for names, driver’s license numbers, and license plate numbers, but the queries also alert the officer to potential hazards such as stolen vehicles and wanted persons. MDC is often integrated with CAD, mapping options, and automated vehicle location (AVL). MDC requires an “always connected” wireless connection between the vehicle it is in and the central server.

Field reporting consists of allowing officers to fill out common forms using the computer on location. The simplest implementations of field reporting require that the report is then printed and processed using the same method as a handwritten report. A slightly advanced version allows the reports to be transferred to floppy disks or thumb drives so the data can be transferred to the central database. More advanced systems further automate workflow with online routing, approval, revisions, and status reports. They are closely tied with the RMS.

Other Associated Technologies
Other associated technologies that can be added on to further advance mobile computing for law enforcement include magnetic stripe and bar-code readers, digital cameras, printers, fingerprint scanners, handwriting recognition, and voice input.
Purchasing Guidelines, Cost Estimations, Training, and Other Considerations

When it comes to planning for the purchase of mobile technology, there are many factors to consider including technological, administrative, cost, process, and personnel issues. Creating a complete Request for Proposal (RFP) is highly recommended.

When it comes to budgeting, officials should realize there are many short and long term budget considerations; they must plan for all related costs including training, support, consumables (i.e. paper and toner cartridges), and wireless service fees. It is important to consider that the industry standard cost estimate for application maintenance is 17 to 20 percent of purchasing costs. Additional money must be set aside for hardware maintenance and replacement. Maintenance costs will likely go up over time.

Some high-level ideas to keep in mind while planning include:

• Prioritize your requirements to reflect what your agency needs most.
• Set appropriate expectations for the project from the onset. Commit goals, objectives, and project scope to paper from the beginning.
• A formal functional specifications document and technical specifications document should be prepared to properly plan such a project.
• A rollout schedule for implementation should be developed.
• Training, system documentation, and security issues should also be properly planned and committed to on paper.

Other helpful things to consider include:

• Look to other agencies to learn from their experiences
• Attempt to create economies of scale by purchasing products in conjunction with other groups
• Be sure to get initial user input and on-going user feedback
• Don't overlook ergonomic and safety issues in your plans

Perhaps the most necessary and most often neglected element of such a project is training. It is a well-known fact that no system can be truly successful if its users are not properly trained. There are many practical options available for training, including computer and web-based offerings and classroom training. Many vendors provide training as part of their services. Reference materials for applications and equipment should be readily available to staff. Ongoing follow-up and training should be planned for with the deployment of a mobile computing system.

Developed for IACP’s Technology Desk Reference, 2006 by Margaret Jacobs, Consultant
A Perspective

By Gary Allen

In the past 10 years, municipal police departments across the United States have been deploying wireless networked laptops in patrol cars. Large and small police departments like the Miami, Florida; Sacramento, California; Baltimore, Maryland; Philadelphia, Pennsylvania; and Henderson, Kentucky have installed wireless networked laptops in the hundreds and the list goes on. These city based police departments have outfitted hundreds of their police vehicles with mobile data retrieval from a central location.

At the same time, smaller police agencies are also seeing that laptops are becoming standard vehicle equipment for their officers. In the small, southern New Jersey town of Lumberton, Lieutenant Jeff Smith says that his department, which serves the policing needs of Lumberton and surrounding towns, has 12 of its officers equipped with laptop computers using a digital Code Division Multiple Access (CDMA) service in their vehicles.

In 2006 the Lumberton Police Department began using the laptops for data entry (electronic, paperless forms), as well as for the search and retrieval of information. An example of how this might work: the dispatch center at the Lumberton PD receives a complaint (noise) and immediately opens a case file and communicates that information to the appropriate officer. Once the officer completes the investigation the appropriate information (narrative) is entered into the officer’s laptop. The completed report is then sent over the digital wireless network back to headquarters. A supervisor, upon receipt of the report, conducts a review. Once the review process has been completed the report is electronically sent to the county central database in another city, Westhampton. All backups of public safety data within Burlington County are handled by the county information technology office.

Sonina Matteo
Tech Research Services
Law enforcement agencies, fire and EMS agencies thrive on information—they need it to respond to emergencies, anticipate what they’ll encounter when they arrive on-scene, and to help predict incident trends and patterns. Before computers, information was gathered by officers in the field, transmitted to others via paper notes, reports and other handwritten notations, and then filed in metal cabinets. Now the computer has taken over routine data collection, transmission and distribution at most of America’s law enforcement agencies, including transmitting data to mobile units in the field.

Along with the computerization that began in the 1980s, a few large agencies began installing specialized mobile computer terminals (MCTs) in their patrol vehicles. At that point mobile data was defined by proprietary, small-screen (30 lines x 24 chars) terminals and agency-owned radio systems, supplied by just a handful of companies that specialized in mobile data. These turn-key, radio-and-terminal solutions did the trick, but were expensive, time-consuming to implement, and generally unreliable. The displays were also very limited in the type of data they could transmit—text-only on small screens, with non-ergonomic keyboards.

The mobile data networks used radio systems built and maintained by the law enforcement agencies themselves. They required a dedicated radio channel and moved data at very slow speeds. But since the data usually consisted of very brief text information, the networks were generally sufficient for officers in the field who needed basic information access.

In the 1990s, commercial applications for mobile data began to appear, especially among package delivery and service companies that needed to efficiently manage their fleets. Consumer applications for mobile data began to appear in the form of alphanumeric pagers, personal digital assistants (PDA) and even cellular phones via text messaging. Suddenly, the proprietary nature of mobile data disappeared, replaced by scores of companies offering both individual components of mobile data and entire end-to-end networks that could span the country.

Now, in the 21st century, mobile data is common among ordinary consumers and in every size of American business—there are dozens of PDAs, cellular phones and laptops that can transmit data wirelessly from anywhere. Everyone from teens to corporate executives can check their e-mail, stock holdings, bank accounts and sports scores using wireless data applications.

But adoption of these advanced wireless data technologies has been slow to come to public safety agencies, including law enforcement. These agencies are limited by tight budgets, and constrained by the complexity of linking to records management and computer aided dispatch (CAD) systems, and the requirement to deploy completely secure and reliable data links with criminal justice databases.
Large agencies have usually had the resources and technical expertise to deploy mobile data systems to support their field forces. Sometimes these networks are implemented by large system integrators under a contract that includes a voice radio and computer data systems. Smaller agencies must usually depend upon outside experts to design and install mobile data systems, usually as part of a purchase of records management or CAD software.

Commercial wireless networks offer a quick, simple and inexpensive mobile data solution for large and small agencies. For personal communications, hundreds of agencies have deployed Blackberry or similar wireless PDA devices to allow transmission of text information to key personnel either via paging or e-mail. Cellular telephone carriers also offer a mobile data solution over their data networks that mirror their voice network coverage. Early networks used technology that offered no great speed advantage over private radio systems. However, using the cellular network eliminated the design, construction, and maintenance of a private network, and in most regions provided improved and more reliable mobile coverage.

Early cellular data networks (CDPD) piggy-backed on the voice network, and sometimes suffered from congestion as network traffic increased. More recent, so-called third-generation (3G) technologies (1x-RTT, GPRS, EV-DO, EDGE, etc.) are operated separately from the cellular voice network, and have increased speeds as well.

As large and medium-size agencies have successfully implemented mobile data over the past five years, law enforcement officials recognized the advantages of having access to data from the field. This, in turn, has generated interest in so-called “broadband” applications for mobile data, including video, mug shots and other photos, fingerprints, in-field reporting, and sophisticated ad hoc networking and messaging at critical incident scenes. Just like consumer DSL and cable access to the Internet, law enforcement agencies want instant access to complex information anywhere within their jurisdiction.

In the wake of the terrorist attacks on September 11, 2001, the Federal Communications Commission (FCC) recognized the need for additional spectrum to allow broadband data communications. They allocated 50 MHz of spectrum in the 4.9 GHz band exclusively for public safety mobile or hotspot mobile data networks. The band is adjacent to the consumer Wi-Fi wireless data band, and the equipment operates using well-establish technical standards that allow broadband transmission speeds.

Some agencies have created hotspot mobile data networks using this new band or the standard Wi-Fi band. They have placed base stations at strategic locations around the jurisdiction (headquarters, gas pumps, parks, etc.) to allow officers access to the network when they’re within range so they can upload reports from the field and download reference information. Some jurisdictions are small enough that they have been able to create city-wide Wi-Fi networks to allow broadband communications from anywhere within the city or town.
More recent developments allow the creation of a so-called “mesh” network using Wi-Fi access points scattered around the jurisdiction. A receiving base station relays data from a field unit on to another base station, and the process repeats until it’s received at the main base station. Out-going data is transmitted to the field unit the same way. The method has the advantage of broadband speeds and lower network deployment costs.

Most recently, several companies are offering computer-to-computer messaging applications that use the Wi-Fi and 4.9 GHz band. The programs allow instant messaging, multiple streams of and audio video between several computers, and unit management features to handle a critical incident.

Several companies offer multi-path networks that select the best network among those available and route the field unit’s data appropriately. The software’s intelligence can locate and use the agency’s own radio network, a cellular network or a nearby Wi-Fi access point to create a constant data link for the field officer. As of mid-2006, several companies are developing wide-area Wi-Fi technologies that will provide broadband speeds over tens of square miles. At the same time, several cities in the U.S. are considering the deployment of free, city-wide Wi-Fi networks. Both of these developments could allow public safety agencies another option in achieving wide-area, broadband mobile data capabilities for their field forces.

At the same time, cellular companies have mapped out ever faster data networks for the future, with some companies promising speeds up to 5 Mbps within the next two years, faster than traditional wired DSL service.

The nation’s law enforcement agencies generally use one of these mobile data solutions:

• Slower-speed networks which the agency must build, operate and maintain. The trend towards regional radio networks, including 800 MHz trunked systems, has made this option more feasible, particularly for smaller agencies.
• Higher-speed cellular data networks operated and maintained by cellular carriers. This option is excellent for small agencies in well-covered cellular regions, since there is little up-front cost and there are typically fewer units for which to pay a monthly access fee.
• Self-built Wi-Fi networks for computer-to-computer or computer-to-base networks, all installed and maintained by the agency. This option provides full broadband data speeds, but with very limited range unless the jurisdiction is very small.

Within each option the challenges remain basically the same as the 1980s: initial and ongoing cost, reliability and speed of transmission.
Basic Questions to Ask When Considering Mobile Data

- What information do you need to access from the field: basic text (vehicle registrations, etc.), high-volume text (in-field reporting, records management, CAD, etc.), or broadband (photos and other graphics, video, fingerprints, etc.)?
- Can you depend upon a cellular carrier for network service, or should you build your own mobile data radio system, either standard radio or Wi-Fi/4.9GHz?
- Do you need a proprietary data terminal for only mobile data, or do you need to use a ruggedized laptop for other applications such as word processing?
- How and where will the network terminate: at the your agency’s local server, through the Internet to a server, at the county/state interface to NCIC, etc.?
- What applications will be available on the network: RMS, CAD, links to warrants and vehicle registration databases, automatic vehicle location (AVL)?
- Do you need mobile data access only in vehicles, or also portable, handheld access?

Developed for the IACP’s Technology Desk Reference, 2006 by Gary Allen, editor of DISPATCH Monthly Magazine.
http://www.911dispatch.com
Benefits to the Community and Agency
By Paul Wormeli

A successful mobile computer implementation offers many benefits to the agency and the community. Depending on the applications used, efficiency, accuracy, public service, and officer safety can all be enhanced by the mobile computer solutions.

After transitioning to a mobile computer solution for dispatching calls, sending messages, and running information and wanted checks, an agency will see a tremendous reduction in the amount of voice radio traffic. The transmission of routine messages and checks on vehicles and persons by computer allows the airwaves to be clear for emergency messages. Citizens benefit from faster stops with the elimination of lengthy delays waiting for checks to be completed. Dispatches and lookouts are delivered with complete information, there is no need to repeat or confirm addresses or descriptions.

Replacing paperwork with electronic reports and forms can allow for greater efficiency for the officer taking the report and also many others. Once familiar with the electronic system officers can move quickly through the data elements of a report; narratives become more detailed and better organized because the author can use word processing functions such as copy and paste to move sentences or paragraphs. Handwriting is no longer a hindrance to those reading the report, including data entry clerks, detectives, and prosecutors. A well designed system will import the report directly into the records management system. Data entry personnel then change their focus to data verifications, ensuring that reports are even more accurate than ever before. Hiring temporary data entry clerks or staffing with overtime is no longer necessary because of the instant transfer of data. Finally, this data is immediately available for investigative use rather than backlogged waiting for entry by overworked staff. Getting useful information while in the field can make the difference when a case is rapidly evolving. Electronic reports are the cornerstone of a good information system.

Using the computer as a data dissemination tool is an emerging trend in law enforcement and it allows for fast and accurate information management. The traditional method of printing bulletins and posting them in the station can be replaced by a virtual roll call through a web based interface. This uses point and click functions similar to the Internet that many are already familiar with. The officers get up-to-date

(Continued)
Benefits of Mobile Computing

The classical approach to building information systems in law enforcement has been to design what is most often called a records management system. The very use of this term illustrates the underlying premise in the design and construction of the system; namely, to take some portion of the manual records stored in a records room and duplicate them on a computer. The justification for duplication of these manual records in a computerized form is that it is easier and faster to count the crimes that occur for Uniform Crime Reporting (UCR) purposes, and that it is possible to search and find the records faster and with more flexibility than by going through paper files.

When technology, policy, and training come together, mobile computer applications allow for more efficiency and ensure that the officers spend more time on the patrol. Departments implementing a system can use time studies to measure some of the basic system components, such as the amount of clear air time once computerized messaging is available as compared to a similar time period prior to implementation. But many of the qualities of a good system are hard to measure, such as the rapid capture of an armed and dangerous suspect because the photograph was electronically transmitted to the officers. The ability to research a suspect from the street and complete more thorough investigations are important to officers and detectives, but hard to track. These types of examples can be gathered over time, and can often be more compelling than simple time savings measures. Finally, the satisfaction of the users can be measured through surveys and interviews. Some of the best enhancements to the system can be discovered and implemented based on comments from the people who use it every day.

Sergeant James Craige
Alexandria Police Department—Virginia

Information on wanted suspects, missing children, crime trends and policies. Through this information the officers are able to self direct patrols to target trends immediately, and have a vast amount of resources in one location. These bulletins can be instantly changed or rescinded. The result is a better informed officer who is aware of the problems in the patrol area and able to respond better to the citizen's needs.
on the quality of the design and implementation, the results of automation may be more frustrating than the paper-based process it intends to support.

New Models in Information Technology

Today’s thinking in information technology provides a number of new models which can be helpful in the design of law enforcement information technology. Contemporary thinkers have suggested that the design of modern information systems must be intricately linked to the processes that such technology is designed to support, rather than simply automating paper records. Further, the re-engineering of these processes should be a predecessor to defining information technology applications, so that we do not simply automate what exists. The automation of a flawed or unnecessary process results in a faster bad process.

This paradigm shift in the development of law enforcement technology offers a unique opportunity to redesign applications from the perspective of the law enforcement processes rather than from the mere desire to computerize manual records. One of the major implications of such a new approach is that agencies are taking a fresh look at the processes in which field personnel are engaged, with a view toward using technology to make these processes more effective by providing improved tools for the field officer. Designing technology from the viewpoint of the field results in very different kinds of software applications than have been implemented in the conventional CAD/RMS systems that have been created over the years.

Such a field-based computing perspective is particularly compelling now because of the introduction of mobile computing technology that is reliable and economical. It has only been possible to consider this perspective in the last decade, and perhaps only now, in 2006, has there been enough breakthroughs in communications technology to support the more ambitious implications of field-based computing.

Given the advent of the new capabilities of mobile computing, it is important to define in advance how this technology can support the increased effectiveness and productivity gains sought by law enforcement executives, and the new models of policing that have emerged in recent years. The potential benefits of using this new approach are fundamental to making decisions to deploy this technology or to make it a part of an agency’s information technology strategy. The intent of this article is to document the real-world benefits of mobile computing and its extensions to the law enforcement mobile office to make clear the ultimate value of this technology. The use of the term real-world is intended to imply that the benefits described here are not features of technology, but rather a compendium of what this technology can do in actual law enforcement practice to add value to the processes it supports.
The Mobile Environment

Mobile computing in law enforcement covers a host of alternative technologies. With respect to the hardware, the technology includes handheld computers, the so-called “tablet” computers (primarily pen-based), and full size notebook computers with attached keyboards (with or without pen input). In software, mobile computing includes simple mobile digital terminal emulation (messaging, NCIC access, etc.), field data reporting, the development of a field knowledge base, and the associated software for interfacing and message switching. Additional supporting software may include mapping displays, handwriting recognition, and voice recognition for dictating narrative components.

In addition to the mobile computer and associated software, there are a number of supporting technologies that can be employed to further enhance the value contributed by the use of mobile computing technology. Given the existence of a mobile computer in the field, add-on technologies can include automatic vehicle location (AVL), magnetic stripe or bar-code readers, digital photography, field printing (such as for citations or reports), fingerprint scanners, and voice input.

General Benefits

The broad general benefits that can be achieved with mobile computing technology are really a function of the combination of hardware and software deployed, and the supporting technologies used. However, we can explore the basic benefits achievable by assuming that a typical system would include mobile communications (with dispatch, queries to NCIC, local messaging) and field data reporting (incident, accident, field contact, etc.) Given this specific implementation, the following benefits can be realized.

Reduced Radio Congestion

The use of digital technology to make queries, respond to dispatch calls, report status changes, and handle digital car-to-car messaging will reduce radio traffic by anywhere from 10 to 40%. To confirm this figure, try capturing a day of radio traffic in any typical police agency and look at the transactions by type. You will find that the bulk of the traffic falls into one of the above-mentioned categories. Many agencies estimate up to a 50 percent reduction in radio traffic following the introduction of mobile computing.
Lighter Dispatcher Workload
This benefit is a function of how the communications center is organized, but there is no question that digital technology reduces dispatcher workload. Even with a good CAD system, without mobile computing the dispatcher must make status entries into the CAD system, issue call assignments on the radio (with occasional repeats), and make state/NCIC inquiries and pass the results back to the inquiring unit. All of these activities can be performed by officers in the field using mobile computers rather than by dispatch personnel.

Many agencies use a dedicated information channel which is separately staffed for this purpose. With such a dedicated position, the use of mobile computing for this function can save the typical 5.2 persons it takes to staff one full-time position. For agencies using cost savings as a justification of mobile computing, it is easy to calculate a savings of $30,000 per person (including fringe) times 5 persons times the life cycle of 5 years for this technology to show a cost savings of $750,000 for this change alone. Furthermore, there are equipment and floor space savings associated with reducing dispatch staff as well as other overhead that could easily save another $50,000 per year. The resulting total savings could be as high as $1 million or more over five years, just by saving the cost of this one position.

Improved Supervision and Resource Management
With the mobile computing messaging capability connected to a CAD system, field supervisors can easily know what call their units are assigned to, revise assignments as appropriate to ensure that the best available resources are sent to each individual call, and know when the available staffing is likely to be insufficient. Sergeants in the field can override the dispatch assignment (if they are allowed to do so) to achieve more effective utilization of their resources.

Cost Savings by Avoiding Paper
The product of police work is paper. Incident, accident, arrest, field contact, citation and other documents are the physical end result of many law enforcement processes. With the use of field-generated, computer-based reports, it is possible to eliminate the generation of the original paper form. Paper need not be the medium of information exchange within the police organization itself. Once this new paradigm is accepted, there are serious cost savings avoiding paper as the communications medium; for example:

- Copying supplies (paper, toner cartridges and other printer supplies)
- High capacity copier machines
- Labor costs to make and distribute copies
- Labor costs in filing and retrieving paper records
- Storage space, filing cabinets, floor space required to maintain paper copies (not just in records but in all the duplicate file cabinets maintained by detectives, the chief’s office, etc.)
- The cost of lost, improperly filed, or damaged paper reports
- The cost of printing forms
Less Time in Data Transformation
In a paper-based system, the field officer captures the required data on a paper form. It is at this point that the most knowledge about the event exists, and it is the officer filling out the form who has the best opportunity to initiate the capture of reliable and accurate information. Yet with the paper-based form, police agencies typically expect records clerks to resolve ambiguities and correct errors in UCR classification or otherwise repair the work of the field officer. Further, the records clerk recaptures the data a second time by keying in the critical information into a records system. Not only is this process redundant, but it also has the potential to introduce errors by simple transposition or other variations from the original. This process costs time and money.

In a records system where the records clerks are entering the full incident report (as opposed to simply enough data to meet the old UCR standards and to do a few batch reports), a typical data entry measure would be minimum 20 minutes per report. Multiplied by the number of reports entered per year, and computing the five-year savings if this function is eliminated by having the data more accurately and completely entered in the field, the resulting savings are substantial. As an example, an agency processing 10,000 incidents per year would expect data entry to cost $225,000 over a five year period (10,000 times 0.3 hours per report times $15 per hour times 5 years).

To be conservative in this calculation, it must be recognized that some amount of quality assurance is still needed even with the best software that does full editing and data validation in the field, so that the full savings may not accrue. However, quality assurance reviews should take no more than 15% of the time it would have taken to actually reenter the data, so we could multiply the above calculated savings by .85. The potential savings is then $191,250 over a five-year period. Combine this figure with accidents, citations, field contacts, arrests and other reports, and the savings start to mount. In many instances, this single benefit of mobile computing will justify the investment.

Reduced Cost for Required Changes in Reporting
When state or federal changes to reporting requirements are mandated, such as with the introduction of the National Incident Based Reporting System (NIBRS), mobile computing software will be less costly to change than all the manual forms and processes that are in place. Adding a few data elements (such as the arson reporting changes) is much easier in a well-designed computer program than the cost of remaking all forms. The traditional form approach involves labor intensive work in redesigning the form, printing, implementation, and retraining. Often the computer equivalent can support a change without this extensive labor cost.
Elimination of Transcription Errors
Good quality mobile computing software will include edit rules to validate data as it is captured at the point of origin. Using lists of options, check boxes, and built-in edit rules will reduce the opportunity for error and improve the quality of the ultimate record.

Lower Training Costs
Experiments in the use of mobile computing in police agencies quickly reveal that it is very easy for officers to adapt to the computer-based approach of capturing data. A well designed, Windows-based software program for incident capture will include on-line help features, built-in edits to instantly detect errors in entry that can be immediately corrected, validation of entries in multiple fields, and other feedback mechanisms to shorten the time it takes to train officers to use this medium. Particularly for pen-based mobile computing, the metaphor of the clipboard is maintained in the data entry process, and the computer screen appears to the officer to be very similar to the manual form.

Less Elapsed Time for Investigative Response
Several studies have established that the probability of closing a case by arrest decays as time passes. The mobile computing entry of full case data enables the near real-time transmission of the case data to the investigator who is assigned and minimizes any delay of the follow-up investigation.

Improved Data Integrity
It is intuitively obvious that data captured in the field at the source will be of higher quality than data entered from manual forms after the fact. The quality of the data improves directly in proportion to the quality of the edits built into the software on the mobile computer; extensive conditional edits and validation rules requiring correction before uploading data lead to a significantly lower error rate and greater database integrity.

Improved Officer Safety
A fundamental objective for mobile computing is to provide the officer with a means of determining if persons are wanted or are otherwise a danger to the officer. High-speed access to local, state, and federal databases provides this capability from the field. Hardware and software used in mobile computing can also provide a function key or other means for the officer to initiate an alarm indicating that the officer needs help without the knowledge of the person endangering the officer.

When the mobile computer is connected via a radio network and an automatic vehicle location (AVL) receiver is added to the vehicle installation, the system can transmit the location of a vehicle to an accuracy of up to 10 meters with differential AVL capabilities. An officer needing help can be located by the dispatcher even without a verbal message defining the officer’s location.
Better Resource Utilization
Where an AVL system is employed to inform the CAD system of the exact location of the vehicle, the CAD system is able to select the closest available unit to respond to a call based on the actual location of all units rather than relying on a table look-up to determine which beat or sector should handle a particular call. This approach certainly provides for a reduced average response time and therefore a more productive response force leading to the handling of more calls per unit than is otherwise possible. The deployment of AVL added to a mobile computing solution raises interesting questions about the whole concept of beats as a means of pre-positioning units to respond to calls for service. Some cities have estimated that the implementation of this concept could result in the equivalent of a 10 percent gain in the effective patrol force.

Higher Report Quality
It is easier to capture and include data in a report that is produced on a computer than one that is written by hand, assuming that the software is well designed. In a Windows environment, for example, officers can use a pen or other pointing device to check off boxes, get help on fields, and spell check narrative entry.

With point of origin editing and validation, the final output of the reporting process will improve over manual means. The report generated on a computer can also be printed on a high quality laser printer, adhering to state or other standards for formatting. Closely associated with the improved report quality is the proficiency of the officers using the system. In reporting on the study conducted in Los Angeles on the value of mobile computing, the National Institute of Justice found that “the more reports an officer wrote with the computer, the faster he or she could produce them.” As the proficiency increases, so will the quality of reports created in the field.

Improved Organizational Communications
Mobile computers connected through a radio network create the potential for the use of electronic mail between cars in the field and to any e-mail recipient in the department. With e-mail systems, many of the routine organizational communications that previously required meetings are no longer necessary, freeing people to do more productive work and minimizing the time spent in verbal communications or in writing memos. The result of all of this is movement of information throughout the organization at a much faster pace with greater accuracy and integrity.

Support for Community-Based Policing
Computer support for personnel in the field opens many new doors to support for field activities embraced by the community-based policing model. With the mobile computer, it is possible to put in the hands of the officer on the scene support tools such as standard operating procedures, penal codes, lists of community contacts and business contacts, and lists and phone numbers of support services that can be applied in proactive policing.
intervention strategies. In addition, many agencies have found ways to increase the number of officers involved in community-based policing activities by applying the labor saved through using the mobile computer directly to increased community-based policing activities. This analysis has been the basis of grants given to agencies under the COPS MORE program.

**Increased Officer Confidence**
There is no doubt that having a store of information available to help make decisions will increase the confidence of the decision-maker. The concept of a field knowledge base with information needed by an officer readily available on the officer’s notebook means that the officer truly is armed with information that may mean the difference between deferring the resolution of a problem and solving the problem at the scene.

**Enhanced Professional Image**
The use of advanced technology, particularly specialized hardware and software suited to the police environment, such as pen-based solutions, indicates to the community that the officer is well equipped to be of assistance. This same image indicates to the suspect that the officer has the tools to find out whatever is important about the individual at hand. These impressions will create increased community confidence in the patrol force.

This list of benefits from the use of mobile computing is largely independent of the technology employed. The benefits are there regardless of whether laptops or pen-based computers are used, or irrespective of hardware features other than assuming the hardware is adequate for the work implied to achieve the benefit. However, there are benefits that are quite specific to particular technologies that may be employed in law enforcement mobile computing.

**Officer Specific Technology Benefits**
An example of a technology that adds specific operator benefits is the use of pen-based computing. Of the mobile computing alternative technologies, pen-centric (designed to use a specialized pen as the input device) hardware and software offer a special set of advantages. Pen computing essentially replaces the mouse or other input device (including the keyboard) for data capture. The pen as an input device has these advantages:

- Allows the user to more directly point and select from a drop-down list than a mouse does. Less hand-to-eye coordination is required to position the pen on the proper entry field as compared to the use of a mouse, leading to faster completion of reports.

- Permits the operator to write directly on the surface of the computer and convert it to text readable by the computer. This allows the unit to be used outside of a vehicle without requiring a keyboard. It also allows a more natural communication with the person being interviewed. Field workers in many professions using pen computers have found “that pen tablets and slates disappear like a notepad or clipboard, and that the devices help them maintain the eye contact they desire while taking reports.”
Mobile Computing Technologies: Benefits

- Sustains the familiar clipboard metaphor for filling out incident and accident reports, and thereby reduces training time and increases proficiency in the use of the system.

There are other specific technologies that can enhance the value of the mobile computing approach. For example, the use of time-saving devices such as magnetic stripe readers or barcode readers to instantly capture driver identification from the encoded driver’s license will have a potential impact on reducing the time it takes to complete a report.

**Operational Impact**

There are other benefits of using mobile computers based on more than the technology itself. In particular, for field data entry, that may have a major impact on productivity depending on the nature of current practices for report writing, and the willingness of the department to re-engineer the process and retrain officers in new report writing methods. The benefit is the potential reduction of time field officers spend in the report writing function, which has been estimated to occupy as much as 20% of patrol time. If it is possible to significantly reduce this time by eliminating steps or simplifying data capture, then major productivity gains for the department will emerge. For example, if it is the current practice for a field officer to use a worksheet to capture all of the data relative to an incident report and then to return either to the vehicle or to the office and prepare the final report, the data is actually being “captured” twice. If one of these steps can be eliminated, then there will be time savings.

As another example, of benefits from operational changes, consider the situation of responding to a serious accident involving multiple parties. It is not uncommon for the officer to have to create numerous reports arising from this event, including an accident report, one or more citations, possibly an arrest report, DUI incident report, etc. With manual forms, many items of data on persons, vehicles, and locations are duplicated on different forms. If the mobile computing software allows this data to be captured once and reused on different output forms, there is no doubt that time savings will accrue. In many cities, the time spent handling an accident averages 90 minutes, largely due to the extensive paperwork. If this average could be reduced significantly by eliminating duplicate data capture and speeding the data capture process, major productivity gains are possible.

**Summary**

The potential for mobile computing to result a 30 percent increase in the available resources of the police department is within the reach of a carefully designed implementation. The work saved by the reduced data collection and entry time and the reduction in the infrastructure needed to support a paper-based operation could achieve this objective. Acquiring the assets of the mobile computing infrastructure is an investment that can have long-lasting returns.

Written by Paul Wormeli, Executive Director of the IJIS Institute for IACP’s Technology Desk Reference, 2006. Further reproduction without express written permission is strictly prohibited.

http://www.ijis.org
How Mobile Computing Works

By John Dewey

This section is included in the TDR to offer chiefs a brief introduction to Mobile Computing. This section is designed to give executives a basic understanding of the technology system they are considering for purchase, and is not designed to be a comprehensive review of all technical considerations.

As law enforcement executives develop technology systems to meet the needs of their specific agencies, additional information on the benefits and considerations of future pieces should be sought. This section is written to help non-technical persons understand the basics of how systems work, the meaning of common terminology used, and the implications of choosing one technology over another.

Every effort has been made by the IACP’s Technology Technical Assistance Program (TTAP) to ensure that this section incorporates the general issues related to mobile computing technology. However, law enforcement administrators should be cautious that no primer can meet all the needs of any given law enforcement agency. Each agency needs to tailor its research to its unique technology needs.

Mobile Computing

Simply stated, mobile computing is the deployment of industry standard portable computers in a law enforcement patrol fleet.

Portable computers installed in patrol vehicles are a small component of a complete mobile computing system. The function of computers in patrol vehicles is determined by the application software deployed as part of a complete system.

The most common applications for a mobile computing system are mobile data communications and field reporting. While both of these applications can coexist on the same in-vehicle computer, there are differing requirements for the infrastructures necessary to support these applications on a fleet wide basis. In particular, the MDC application requires an “always-connected” wireless connection between the vehicles in the fleet and a central server. On the other hand, a field reporting application does not require a constant wireless connection to a server and in fact may use methods other than wireless communications to transfer information between the mobile computers and the central server.
Mobile Data Communications

MDC is the most popular application of mobile computers in law enforcement. A MDC system gives law enforcement personal nearly instantaneous access to vital information collected in various law enforcement databases. A MDC system can simultaneously access local, regional, state, and federal databases from a single query.

The most common queries are based on vehicles tags, operator’s licenses and person names. Besides providing details on vehicle and operator licenses, replies can notify the officer immediately of any potentially hazardous situations such as known felons, wanted vehicles, etc.

A MDC system is often also interfaced to agency’s CAD system. Such an interface allows a dispatcher to send dispatch message directly to a unit’s mobile computer. Officers can use the MDC system to record status changes and exchange messages with dispatch personnel.

Most MDC systems include integrated mapping. The map display can be used to pinpoint incident locations and in some cases even give driving instructions. Map displays can be enhanced with AVL providing users the location of all vehicles in the fleet.

AVL used to be an expensive application. However, since AVL can share the same infrastructure with an MDC system, the cost is only incrementally more than a MDC system without AVL.

Field Reporting

Mobile computers can be used for the preparation of field reports. Field reporting is the second most popular application of mobile computers.

The simplest field reporting systems use familiar forms that can be completed using the mobile computer. These forms are then printed in the police station. The printed forms are then processed using the same workflow of hand written reports. The completed reports can be transported from the mobile computers into the station using a variety of methods. A wireless solution is not required. The simplest systems use floppy disks or “thumb drives” to transfer the data from the mobile computer to the in station server.

More advanced field reporting systems can automate the workflow of reports. Reports are routed as necessary for approval and can be returned to the originator for revision. Online reports are available to review the status of reports and notify of outstanding and/or overdue reports. Since these advanced systems often require close integration with an agency’s RMS, they are most often supplied by the vendor as the RMS system.
Benefits of Mobile Computing

The benefits of a MDC system derive primarily from giving officers immediate access to critical information. Officer safety is enhanced with immediate alerts of hazardous conditions that can arise in even routine activity such as vehicle stops.

The community is served by allowing information to be disseminated to officers in a timely and reliable fashion. Be-on-the-Lookout (BOLO) and Amber Alert messages broadcast via a voice radio system are often missed when officers are busy and/or out of their vehicle. BOLO and Amber Alert messages sent via a MDC system are retained at the mobile computer until the officers have seen them.

The workload on dispatchers who would normally handle query requests can also be significantly reduced. Relieved of routine query traffic, dispatchers now have more time to dedicate to critical tasks.

Field reporting can facilitate more complete and accurate reports. With automated field reporting workflow, the timeliness of reports can also be enhanced. Clerical labor necessary in a manual field reporting system can also be significantly reduced.

Equipment Options

Mobile computers used in law enforcement normally fall into one of three classes, each with its own advantages and disadvantages.

Consumer Grade Laptop Computers—These are the least expensive solution. However, since they are not designed for the harsh patrol vehicle environment, they will also have the shortest life cycle. The overhead associated with frequent repairs must also be considered. Perhaps most significant, consumer grade laptops simply are not readable in the bright sunlight often experienced in a patrol vehicle environment.

Ruggedized Laptops—The computers are suitable for the mobile environment. Most vendors offer sunlight readable screen at least as an option if not standard. A touchscreen can simplify the computers use in the mobile environment. A ruggedized laptop may be two to three times more expensive than a consumer grade laptop but given the additional functionality and increased life cycle, that increase is often easily justified.

With either consumer or ruggedized laptops, careful attention must be made to the vehicle mounting solution. A poorly mounted laptop can be a serious hazard in a collision. Interference with the vehicles airbags must be considered.

Fixed Mounting Vehicular Computer—Finally, there are several vendors that offer computers specifically designed for vehicular use. These computers are the most vehicle
friendly. Screens are designed to be readable even in direct sunlight and they all offer touchscreens for simple operation. Mounting is designed to not interfere with the vehicle’s airbags. The cost of these vehicular computers is competitive with the cost of ruggedized laptops.

**Wireless Options**

A MDC system requires an always connected wireless solution. This can be provided by a private data radio solution or a public carrier (e.g., cellular provider).

In some cases, the use of a private vs. public carrier will be decided simply by availability. If some areas, the unavailability of radio frequencies will dictate the use of a public carrier. In other areas, lack of coverage by a public carrier will dictate a private data radio solution.

Where both private and public solutions are available, the choice is often made on cost. A private radio solution will require a significant initial capital investment but once that investment is made, airtime is free. Use of a public carrier requires little in the initial capitalization but the monthly airtime charges will be significant.

The cost of a private radio system can usually be recovered in the first 2–4 years of operation when compared to the airtime charges of a public carrier.

Survivability of the radio network in the case of a major disaster should also be considered. Even if a public carrier network survives a major disaster, it could become so congested with consumer traffic that it’s usefulness for data communications would be seriously diminished.

Most field reporting systems do not require a constant always connected wireless solution. Data can be transferred with traditional “sneaker net” solutions. In a “sneaker net,” data is moved manually using portable media such as floppy disks or thumb drives. Thumb drives have recently grown in popularity. A thumb drive is a very small memory stick that can be plugged into the mobile computer. The drives are available with very large capacities allowing officers to maintain all of their reports on their own personal “thumb drive.” They can use their personal thumb drive to carry reports both from a mobile computer to the in-station server and also from vehicle to vehicle.

Wireless hotspots can also be used to create temporary wireless connections when an officer needs to transfer data between the mobile computer and the in-station server. These hotspots, based on 802.11 wireless technologies, can be strategically placed at headquarters and other locations such as substations, fire stations, etc. so an officer would not have to travel far to transfer data.

Developed by John Dewey, President of PST Technologies, Inc. for the IJIS Institute, 2006. Further reproduction without express written permission is strictly prohibited.

http://www.ijis.org
Things to Consider

By Michael J. McDonald

Mobile computing technologies offer many benefits to law enforcement agencies. There are however, many things to consider prior to implementing the use of mobile computing. Administrators must consider the time, logistics and costs associated with training, vendor support and development of agency resources to maintain this capability. Continued support of this effort and constant analysis of its application is certain to provide a beneficial impact to your law enforcement mission.

Captain Joseph C. Flagler
New York State Police Department

Things to Consider When Acquiring Mobile Data Solutions for Law Enforcement

A fair amount of research and planning will save the agency from making mistakes in the acquisition, implementation, maintenance, and evolution of technology. In no particular order, and by no means an exhaustive list below, are some considerations that should be addressed before, during, and after your project’s life cycle.

- Do not start with a budget. Start with a plan and develop a budget.
- Make sure the budget is adequate for your plan.
- Make sure the budget includes future maintenance, support, and replacement.
- Do you have in-house personnel who have the skill set required for the project?
- Are there other agencies on whose experience you can rely or learn from?
- Is this an initial first time implementation or an upgrade of existing technology?
- Will there be a need for handheld devices or only mobile laptop computers?
- Ruggedized or non-ruggedized units?
- Have you researched where the unit will be installed in the vehicle?
- What are the safety concerns? (e.g., air bag deployment zone)
- What are the ergonomic issues for safe and comfortable use by the user?
- What applications will run on the device?
- How will they be supported? Internally or under contract?
- Will officers be permitted to take the computers out of the car or will they be locked down? Regardless of which choice is made, make sure the units are properly secured while the vehicle is in motion.
- Have clear, concise, and enforceable policies on acceptable use as well
as use of the device while the vehicle is in motion.

• Are there other mobile users in need of an MCT who do not use cars for patrol and can you meet their needs now, e.g., motorcycles, horseback, foot patrol, etc?
• Are their local suppliers for the equipment or the installation of the solution?
• Can you piggy-back off of a state contract for parts, installation, and equipment?
• What operating system(s) should be considered or chosen?
• What are the limitations of the existing or proposed network architecture?
• How will the devices communicate with the host network?
• What solutions have other local agencies decided on and how did they implement them?
• Is the wireless network reliable and proven and will it meet your needs?
• Purchase or Lease? Recommend consideration be given to leasing. ²
• What is the level of user training that will be required?
• What part of each process must be contracted out?
• Is consideration being given to help desk support so as to gain economies of scale?
• Know what applications the devices will provide to your users and know their limitations.
• Try to get a variety of user input for decisions before they are made as often as you can.
• Be flexible in your planning or you will learn to be after the fact.
• Understand that obstacles will present themselves along the way. Do not make decisions that isolate your users or your agency solely on the basis of cost.
• Keep an accurate inventory of all components of the solution selected.
• Educate administration and funding sources as often as possible that technology requires a constant flow of funds and support to make it work. Remember technology is an evolution, not a revolution. You can’t do it all at one time nor can you achieve the pinnacle with just one implemented solution.
• Police officers do not like change. Sometimes you must force change.
• Provide continuous, comprehensive, user training.
• Work with vendors to pilot technologies on small scales.³
• Conduct regular user meetings for improvement feedback and training opportunities.
• Make sure you publicize the benefits of the technology to public, financial supporters, and your administration as to how it is benefiting public safety.
• Make sure your network, hardware, and software provide for a clear upgradable path.
• Ensure network, device, and user security meets the minimum requirements at all levels as outlined in the FBI’s NCIC Security Policy.⁴
• Look to implement solutions in segments providing for small success stories along the way instead of too much at one time.
Mobile Computing Technologies: Things to Consider

- Evaluate solutions practically and not based on user appeal only.
- Do not get overwhelmed. Only address what you can reasonably handle based on your budget and level of human resource support.
- It is recommended that agencies settle on one specific solution instead of trying to support multiple vendor products at once. (Have one model laptop instead of five).
- User support is critical and should not be minimized or haphazardly addressed.
- Have a champion for your mobile solution project and make sure that person is respected and has credibility.\(^5\)
- Get buy-in for your project from the very top from the beginning and prior to any implementation.

Developed for the Technology Desk Reference by Michael J. McDonald, Director of Information Technology at the Delaware State Police.

---

1 Ruggedization is expensive and not necessarily needed. This author believes this characteristic to be oversold in the industry and recommends strong consideration be given to the use of off the shelf laptops.
2 Leasing allows an agency to acquire more units each year and allows cost to be spread out over the replacement cycle instead of all at once up front. Each year's cost is budgeted for and should become part of the annual recurring cost of the project.
3 Vendors like to prove concepts with smaller agencies that are technically strong or who can provide the user base experience they need to market their products. This is an excellent way to acquire low cost to no cost solutions that can add to your suite of products or services.
4 Local agencies may need to rely on state CSA (CJIS Security Agency) for these needs. The current version of this policy is available on Law Enforcement Online (LEO).
5 This is absolutely critical and without it your project will surely encounter resistance from disgruntled users.
Challenges to Implementation

By Jim Craige and Robert Liberati

MCT, in my opinion, has the distinction of being the single most identifiable advancement in the history of law enforcement. Change in policing is never easy, and as much as mobile computing did to advance policing, it is also responsible for considerable resistance by older more seasoned officers.

One of the greatest challenges to the implementation of an MCT program is managing change. At the outset, managing change is the least identifiable as well as the most underrated challenge a manager will have to deal with. Officers who previously have been utilizing the manual processes may resist changes to advanced technologies and will need to see how it can make their jobs easier and safer.

Thus, it is important to try and implement this change to the MCT at the lowest level of understanding. That is to say, do not assume that completing a task on the MCT will be easy or without problems. When implementing, think of the officer(s) who have the most difficulty with technical solutions or applications and gear your implementation to them if at all possible. You must show return on investment. In this case, the officer’s time is the investment and what he or she gets out of it in return is how they perceive the value of that investment of their time.

If you can address this most fundamental issue of user acceptance then every other challenge you face will seem elementary. Why? Because the officers will provide input, try to become part of the solution because, they will have learned to become dependent upon the technology they use everyday and will feel unprepared when they don’t have the MCT to use during an assignment. This would be akin to having an officer go back out on patrol only to find they have left their weapon back at the station.

Ways to overcome other challenges to implementing a mobile computing program may include:

- Take the time to contact other police departments and inquire what lessons they learned when they went through the same implementation.
- Take an inventory of your user requirements and make sure you include real users in developing such an inventory.
- Develop a solution based on your user requirements instead of a budget. The solution should drive the budget, not the other way around.

(Continued)
Early pioneer agencies in this technology sometimes ended up with multiple models of laptop computers, multiple configurations, and sometimes multiple peripherals.

Your best management of such an implementation is when you have one laptop, one mounting configuration, one printer, and one type of an other technology you are implementing.

Keep your options open for future purchases and/or leases of technology remembering that technology should be an evolution and not a revolution. Change should build upon existing technologies.

Know who your business partners are in your implementation solution and make sure they thoroughly understand the Agency’s needs and priorities.

If you have to go out to the market for bidding purposes, make sure your requirements and specifications are well defined and clearly articulated.

Understand that nothing is going to go as easily as planned. Include time in your master implementation schedule for these unplanned issues.

When choosing equipment, make sure your choice can be supported or maintained in the future. Picking a solution that is at the end of its life cycle or no longer supported, will be a cheap initial investment, but will be far more expensive in the long run.

The location of the equipment in the vehicle is critical to both safety and acceptance. Make sure the air bag deployment zone is free from all obstructions and make sure the unit and peripherals are easy and comfortably accessible by the officer. The first installation should not be followed by the second until actual users give their approval of the installation.

Choose a project manager that understands your business and your requirements. They don't have to be law enforcement, but it does help if they are. If you can't get a cop, then make sure the person can understand and relate to officers. Project managers don't need to be technical wizards, they need to know the plan, the vision, and how to manage people and suppliers.

Get the endorsement of your plan and your solution from the CEO of the agency. Leadership needs to publicly endorse your efforts and support the project from beginning to end.

Local police agencies can usually purchase from a state contract and get the same price as a state agency. Use these contracts to your advantage. If you can't, try to combine purchases with other sister agencies so you can obtain the best possible pricing through an economy of scale.

When planning your project, plan down time and catch up time into your master schedule.

(Continued)
• If you are using a vendor, have them do a sample installation of the technology and make sure you have users look at and approve the installation for comfort, practicality, and ergonomics. Don’t complete your installation only to find that officers cannot use the MCT or other installed technology because of where it was placed in the vehicle.
• Conduct user feedback meetings so you can determine if any changes or improvements need to be made.
• Discuss and market your successes to your agency, its administration and to those who funded the project. Try to calculate some return on investment so it can be demonstrated that the money invested was well spent. This marketing will help provide for future funding of other related projects.

Michael J. McDonald
Director of Information Technology—Delaware State Police

Implementation of any new technology system is not without its challenges, and mobile computing is no different. The various challenges and barriers to ensuring a successful technology transition should be addressed during the planning phase of the project life cycle.

Access/Rights Passwords

Agency Inertia, Culture and Training
Change is often resisted, even if there is a known benefit to the agency. Overcome this with adequate testing and training, along with dedicated staff for problem resolution when trouble arises.

Backend Storage
Insufficient backend storage can lead to frustration and expensive future upgrades. Carefully consider the unique backend storage needs of the department as well as accessibility of stored data.

Budget
Under or overestimating budget requirements can lead to perceived added expense and possible decrease future funding. Spend time clearly identifying both the initial investment and recurring costs when developing a budget.
Ergonomics
Equipment should be comfortable and accessible to users. When planning technology changes, consider the needs of the end user.

Staff Resources
Maintenance
Software and hardware may need upgrading and replacement as the system ages. Account for the cost of regular, routine maintenance to keep replacement costs to a minimum.

System Speed and Capacity
Timing
The system may fail if it is put into production before fully tested. Bugs and problems must be identified and fixed before going live or mistrust and suspicion of future technology releases may arise. On the other hand, some agencies have been unable to implement programs because they were waiting on minor fixes to an otherwise functional system. No system will be absolutely perfect. Before implementation a balance must be sought for system acceptance.

Training
There is often a hidden cost of productivity loss during the learning process when converting traditional processes to an electronic system. Recognize that officers who routinely complete reports on time may take longer during their training and the initial implementation of an electronic report writing system.

Troubleshooting
All systems will have bugs and problems. Ensure that extensive troubleshooting and testing happens prior to “going live” to catch as many problems as possible. Also, secure trained assistance for troubleshooting support, especially during the initial implementation phases.

Developed for the Technology Desk Reference by Sergeant Jim Craig, Alexandria Police Department—Virginia and Captain Robert Liberati, Prince George’s County Police Department—Maryland
Estimating Costs
By Jim Craige and Robert Liberati

Planning and purchasing technology involves careful consideration of short and long-term budgeting. Technology costs are not limited to the initial expense of equipment purchase. Recurring expenses, ongoing training and infrastructure support. It is essential that law enforcement agencies carefully account for all related costs must be included when preparing for a technology purchase.

This section lists some of the expenses that should be accounted for when planning a technology acquisition. This list should not be considered exclusive. To create a comprehensive cost estimate, departments should develop a full request for proposals. Additionally, consultants who specialize in mobile computing may assist departments in determining projected costs.

Preparation for Purchase
Each agency should evaluate the need for additional equipment based on the goal of the project. For example, an agency that wishes to complete traffic citations using the mobile computer would need to install a printer in the patrol car. Other agencies may not need this equipment. Hiring an expert consultant who can assist with determining agency needs, drafting RFP’s, and examining vendor proposals may help avoid expensive purchasing oversights.

Initial Investment for Each Single Unit
- **Hardware**—Laptop or mounted computer.
- **Software**—Consider interfaces with CAD, NCIC, MVA, report-writing, car to car messaging, mapping. Computers need not be limited to law enforcement applications; other software such as word processing and presentation software can also be added without affecting the performance of the core applications.
- **Wiring/Electrical System**
- **Mount and Mount Installation**
- **Peripheral Devices**
  - GPS
  - Wireless devices
  - Bar-code or magnetic stripe card readers first year software maintenance, desk bound accessories such as a desk dock for removable computers. Centralized locations may be needed for printing and power in areas like the booking room or report writing area.
Mobile Computing Technologies: Estimating Costs

* Printers-in car or at desk.
* Hubs (MDC storage, RAM, processing speed)

Recurring Expenses
Custom law enforcement software often incurs an annual maintenance fee of around 10–20 percent of the original purchase price. Other software may need updating or upgrading as technology progresses.

- Consumable items such as ink cartridges and paper for printers
- A supply of backup parts, or a turn-key hardware maintenance contract that provides immediate replacement of equipment
- Replacement batteries
- Training for technology support
- Maintenance/service agreement—24/7 vs. next business day
- Software, operating system upgrades

Wireless Infrastructure Costs
Each agency needs to evaluate the available wireless options and budget for the costs associated with them. There are a variety of options, with a variety of costs. They can be broken into two basic categories—agency maintained or commercial systems.

Agency Maintained Option
Would include traditional radio based systems and newer wireless access point systems. The radio systems are primarily low bandwidth suitable for short data traffic such as text messages. The wireless access point systems allow for more broadband applications. Most radio and some wireless access point systems offer coverage throughout the jurisdiction, but not beyond the borders. Some wireless access point systems only offer coverage at strategic “hotspots” in the jurisdiction, leaving large areas without coverage. Some agencies use a combination of radio and wireless access point systems to blend their need for constant data communications and more broadband applications. Maintenance and repair of these systems fall upon the agency. Some agencies may be able to use an existing system of a larger or regional agency. Subscriber fees may be associated with shared use systems.

Commercial Systems Option
Are mostly supplied by major cellular carriers and offer data accounts for each client. Some start-up infrastructure costs may be incurred in order to route the data into the agency network. There is no agency maintenance for the wireless systems, and coverage may include areas outside the jurisdiction and even nationwide. A monthly access fee per computer, approximately $40-80 per computer per month are incurred.
These systems have the capacity to handle both low and higher bandwidth applications. The actual bandwidth achieved depends on the carrier and the services offered in the coverage area of the jurisdiction.

**Training Cost**

Some fee based training may be offered by the vendor. The agency will likely use this opportunity to train the system administrators and the personnel designated as trainers. These people can then train the rest of the agency personnel.

**Additional Costs**

When equipment is purchased, the lifetime of the equipment should be taken into account and budget preparations made for replacement systems. Typical mobile computers last 3-5 years. Most hardware warranties last 3 years, with optional extensions available at additional cost. Some equipment is excluded from the standard warranty, such as laptop batteries and mount parts. These may need repair or replacement in advance of the entire unit.

Developed for the Technology Desk Reference by Sergeant Jim Craige, Alexandria Police Department—Virginia and Captain Robert Liberati, Prince George’s County Police Department—Maryland
Purchasing Guidelines

Source: IACP Law Enforcement Information Management Section

The business processes will need to be adjusted somewhat to accommodate new software. The agency should acquire the product that most closely meets their business process needs within a given budget. There is no “off the shelf” product that will meet every one of the agency’s needs. If the agency adjusts its business process to work with the software constraints, users will be happier and the agency will realize greater benefits.

Set expectations appropriately. Software will not fix all the agency’s problems. If the business process was flawed before the new system was implemented, it will continue to be flawed. Agencies should expect that change will be needed, and plan accordingly. Change is one of the hardest things for agency personnel to accept. The software purchase could be the best solution but because it’s different, it will meet with resistance. The composition of the planning committees is critical to marketing the new system and demonstrating its’ benefits and efficiencies to department personnel.

Agencies should plan for on-going support and maintenance costs. The industry standard for annual support and maintenance of most systems and applications is 17–22 percent of the purchase price. These costs will also rise with time. Agencies should budget for the costs up-front and determine their funding source. Also, it is important to negotiate the maintenance rate during the contract negotiations. Maintenance costs should be fixed for 3–5 years after the first year. The cost for maintenance over several years can meet or exceed the purchase price, if not properly negotiated.

Hardware will also require maintenance and replacement costs. Agencies must plan for this in addition to the 17–22 percent ongoing system and/or application support costs and hardware and software upgrades and replacements. The vendor, consultant, or industry experts should be able to provide upgrade and replacement estimates. These estimates and associated timelines should be discussed and documented prior to the execution of the contract, to avoid any surprises or hidden costs.
Many departments are looking at portable/mobile computing because it is an important element in the development of paperless reporting and, in the long run, may save a significant amount of an officer’s time in the preparation of incident and investigative reports. Portable/mobile computing in the context of this report refers to a variety of technology:

- Laptop or Notebook Computers
- Mobile Digital Terminals (MDT)
- Mobile Computer Terminals (MCT)
- Voice-Based Computer Terminals (VCT)
- Pen-Based Computer Terminals (PCT)

For the purpose of this section portable/mobile computing will be referred to as PPC or portable personal computers. PPCs can be an integral part of the CAD system design, part of the RMS design, or they can be stand-alone reporting mechanisms. Each of these alternatives must be considered in the planning stages. It is preferable for only one alternative to be selected as each requires a different approach in the system design process.

Planning Considerations

Starting the Design and Planning Process

A key set of decisions revolve around who the system users are, how PPCs will be used, and if they will be an integral part of a major system such as CAD. Users of the system must be involved as early as possible in the design and planning process so that they have a stake in the system and viable and acceptable systems are implemented. The following are some potential users of portable computers:

- **Patrol Officers**—Provide the basic input documents to the system. Their participation is vital to assure acceptance and usability of any mobile device. Their participation begins at the CAD level or at the primary reporting level. They require extensive capabilities for officer safety, crime analysis and general criminal information.

- **Investigators**—Utilize the initial crime report and provide the next level of documentation for case details, status, follow-up, and other investigative records required for assembling and filing cases. Investigators may likely use a different type of PPC than patrol officers; however, there should be an interface between the two in order to avoid duplicate data entry.

- **Crime Analysts**—Have a different set of requirements and are concerned with the ability to provide extensive mathematics and graphics to perform complex analysis of crime patterns.

- **Command Personnel**—Must be supportive of the system development process and must also define their needs for the type of information to be provided by PPCs.

- **Technical Personnel**—Are concerned with the design requirements and should translate and analyze the user requirements into viable technical specifications.
Many successful projects use a technical committee and a management committee. The technical committee should be chaired by a user group supervisor and have key technical personnel as advisors. The management committee usually makes the final decisions. Other approaches have included overlapping subcommittees; however, keep the committees small so that decisions can be made in reasonable period of time.

**Statement of Goals and Objectives**
Every planning phase should have broad statements of system goals and objectives. They place boundaries on the system and give the direction for design.

Goals and objectives for PPC usage could take the form of generalized statements of the users’ goals, such as:

- Reduce the costs of report preparation and records management
- Improve the accuracy and utility of information
- Minimize data handling
- Develop consistent chain of reporting and analysis
- Maximize officer time in the field

The usage of PPCs will depend upon the form of report input you are seeking. Do you want the ability of your CAD system to allow for the transmission of incident reports from the field? If you do, then PPCs must be integrated into the CAD design along with the necessary radio channels and bandwidth. Your goal statements should include this requirement.

When the primary and secondary goals and objectives of the system are established and agreed upon, you may start to define the system requirements.

**Scope of System**
The following is a general description of the kinds of capabilities that should result from the use of PPCs and how they will be used in department systems.

**Interface**—Define those systems that will interface to either the input or output from PPCs. Will there be the capability to access state motor vehicle, criminal history, or stolen vehicle systems from the PPCs? What other systems, such as computer aided dispatch (CAD), crime analysis, or crime reporting, will be procured or currently exist that will be able to use PPCs for data input or output? How will the PPCs interface with them? Answers to these questions start to provide the boundaries of the system design, and are necessary to achieve a smooth integration of the new devices within the existing or planned systems.

**Standards**—What standards are established for your mobile reporting function? Will the PPCs be pre-formatted to include NIBRS or UCR requirements?
they be formatted to meet uniform data reporting requirements or state reporting requirements? Are there data security requirements that must be met? Hardware or software standards must be established by your agency in order to provide the necessary support and maintenance. These standards should be designed to an “open system” standard to allow future systems to be added.

**Process Re-engineering**—Utilization of PPCs often provides the opportunity to review an agency’s work flow and report processes. You must determine if you will embark upon a re-engineering effort before you proceed with your system requirements. You use this phase to validate your reporting process and to determine if you will expand reporting at the original input level. You can also determine if the reporting process will require a custom or standard off-the-shelf software solution.

As part of a re-engineering approach, there can be an analysis of the work flow of your reporting systems. Determine if you will continue to use paper files or develop some form of digital and optical records management. These issues should be resolved during the planning phase so that more detailed specifications can be developed for the proposal stage of the project.

**Environmental Considerations**—What is the physical environment in which the PPCs will be used? This factor is most critical for the selection of the most appropriate devices.

PPCs must function in a full range of weather conditions. Temperature variations range from sub-zero to tropical with a variety of humidity conditions. Similarly, the screens must be visible in bright sunlight and in total darkness. To ensure officer safety, there can be no reflection from the computer screens.

If these devices are to be used in the patrol car, you have to define the space available for installation. Indeed, the environmental conditions are the most daunting to overcome in a law enforcement application.

**Schedule for Implementation**
Define the time constraints, if any, for implementation and installation. You must also consider both the technical and administrative constraints to the schedule (personnel, funding, etc.). Other issues to be considered in scheduling include:

- Software and hardware design and installation
- Test plan
- Training plans
- Cut over from manual to automated data entry
- Maintenance and support plan
Research or Benchmarking
Benchmarking is defined as the process of continuously measuring and assessing processes, services, and systems against those of successful departments or companies.

Review the marketplace. Survey the IACP member departments and determine some best practices that exist throughout the country. What agencies are using portable computing devices and what results are they achieving? Are these agencies of comparable size to yours? Are there any common benchmark systems? This benchmarking activity will ensure that you will receive the best design for your application.

Survey the vendor community and investigate the vendor credentials and product history. Does the vendor provide rapid support and help desk response? Is a modern operating system delivered with the PPC device? What is the vendor-installed base? How is the equipment functioning at these installations?

Budget
When preparing the budget, consider as many options as possible. Include growth concerns, basic hardware and software maintenance costs, and operating costs. Ongoing costs for personnel, maintenance, support, and supplies should also be considered.

Inform your vendors of the approximate budget available for acquisition so that they can bid the best combination of their products within your price range. Doing so will promote more effective competition.

A cost benefit analysis may be necessary to sell this system to city management. Your analysis should point out the great benefit to be derived from the use of PPCs including a reduction in personnel time in the preparation and processing of field reports. This reduction results in greater time available for patrol or community policing activities. Additional benefits include greater accuracy and clarity in reporting and faster filing of case reports.

Warranty and Long Term Support/Technology Updates
Consider that all equipment has a 3–5 year life cycle, particularly in a law enforcement environment where the equipment must function 24 hours a day, 7 days a week. Also, most equipment today comes with a standard warranty on repair.

You must be concerned with the development of a comprehensive plan for hardware and software maintenance. This plan should include considerations for backup, routine support, and user training. Elements of the vendor software or hardware warranty/maintenance agreement should include the following:

- Routine support and problem solution by dedicated vendor staff
- Call out procedures for service 24 hours a day, 7 days a week
Mobile Computing Technologies: Purchasing Guidelines

- Off-site backup and recovery of all hardware and software
- Training and refresher classes

In addition, you should consider the issue of technology update. “Moore’s Law” of computer chip technology says that “chip technology capability doubles every 18 months.” This prediction is demonstrated by the rapid change of simple personal computers. PCs have advanced from basic to Pentium which can perform functions. Computer speed increased by a factor of 50. With that rate of change, an agency cannot possibly keep up with technology; therefore, we must be concerned with issues of compatibility, utility, open systems, and maintainability.

If the technology that is available adequately meets your requirements, when the RFP is submitted, then stay with it. Make sure that the equipment or system you buy is maintainable, is not proprietary, and that the manufacturer has longevity.

Specifiation Considerations

The development of specifications and detailed requirements follow the completion of the planning effort. It is vitally important that the agency provide, as specific as possible, a detailed description of its system requirements. In the case of PPCs only, and in order to comply with city standards or budgetary constraints, selecting a specific technology may be possible. However, it is also important to specify what you want to do with the PPC, what problems you want solved, and what future capability you will require.

Functional Specifications

Define what you want to do with PPCs. Generally, you want to be able to collect, store, and disseminate information and reports. PPCs should be as user friendly as possible and be provided with word processing, telecommunications, and/or forms management as a minimum. Mapping, graphics, e-mail and database capability are nice to have, and may be desirable, but are costly add-ons that require sizable amounts of computer memory.

To ensure officer safety, you want to be able to integrate the output of these devices with your existing systems and provide access to state systems. You must also define whether you want stand-alone laptop/notebook computers or mobile units that are part of your dispatch system. Regardless, the standards must be consistent.

The PPCs should provide the ability to use either radio frequency (as part of a CAD system) or modem telecommunications.

Define any requirements for process analysis. Will the project require process re-engineering and will that be performed by the vendor or in-house staff? As part of your requirements analysis, you should review your procedures for report processing and handling to prevent the automation of an inefficient process and provide insight into improvements in operational procedures.
Define the functional needs that patrol, investigation, and crime analysis have for portable computers. Mobile computers should be capable of accepting all types of information, including reports for incidents/crimes, arrests, property, and evidence. This part of the analysis should consider user requirements for an acceptable device that can accumulate detailed reports, documents, and data requirements of each of the operations and administrative units. These units require the ability to produce crime and incident reports, warrants, arrest information, traffic and parking citations, field interviews, intelligence, mapping, etc. PPCs provide users with the ability to enter this information in a form as usable and understandable as possible. Several alternative technologies exist today that allow the input of this data into a mobile device. Each of these must be evaluated in order to provide the one most appropriate for your needs:

**Pen-Based Computers**—Mobile computers that provide handwriting recognition as input to the units. In reality, the machines and the user must be trained. The machine will usually accept carefully printed letters only. The software program used to recognize handwriting is called an “algorithm” and today’s algorithms can be very frustrating to the user. It is better to use handwriting in conjunction with menu driven choices at each stage of the input process. Each menu would include a list of choices for each line of input. This listing would drop down from the menu and allow the user to just pick a selection. Although there has been a great push for these machines, the pen algorithm, because of its inflexibility, has been frustrating to users and, therefore, has not gained large scale acceptance.

**Voice-Based Computers**—Mobile computers that provide voice recognition and translation for input to the units. This technology has the greatest hope for law enforcement as it requires the least amount of officer typing. Recent announcements encourage new voice technology development and should lead to the establishment of standards. However, the technology is still in a relatively early stage of development and requires extensive training by the user in order to obtain a level of acceptability. At the present time voice data entry algorithms require discrete, rather than continuous, speech patterns and has difficulty differentiating background noise from speech. As a result, it is difficult to use in the patrol car environment. Try to get demonstrations first before you commit to purchase.

**Traditional Keyboard PPCs**—The standard type of laptop or mobile computer being widely marketed. These devices can be combined with on-board radios, built in cellular phones, computer docking stations or operated in a stand alone mode. They are most familiar to most officers and can be used for a variety of functions. Some new developments have modified the screens to provide a “touch screen” capability. This allows officers to use extensive pull down menus and then touch the screen for the appropriate choice. All desktop software will run on these models and a variety of applications will have to be designed.
Define the core functionality for the PPCs. Define the critical and basic system needs that you have. What are the minimum functions to be performed? What kinds of reports, software and graphic capability are required? How will PPCs integrate into the current workflow process? What constraints limit the ability to make full utilization of the PPCs? What processes cannot be changed?

In general, we want to use PPCs to perform the following functions:

- Prepare field reports
- Provide site, or person, history data for officer safety
- Access state or national databases (NCIC, etc.)
- If part of CAD, provide the necessary communications interface for dispatching and status reporting
- Ensure a single source of data entry for records management
- Provide graphics for accident reporting and crime analysis
- Have extensive field level edits, eliminate redundant data, and use forced choice entry techniques
- Be able to selectively modify reports
- Possess capabilities such as easy use, content sensitive help, linkages to external data and systems, common image files, data validation, simple documentation

Define the optional functional requirements. What are the options you would like if they can be provided within the bounds of the funds available? Are there special graphics or communications requirements? Detail the alternatives.

**Technical Specifications**

The technical specifications should consider many specific requirements unique to your agency environment, including considerations of sizing, environment, and communications.

System sizing is a function of the type of reporting, graphics and communication software that will reside on the PPC; scalability for future growth; reliability; and redundancy. Sizing more clearly defines the scope of hardware and software technology that should be used by various departments.

Other issues of concern in the use of PPCs include defining the interfaces that are required to other systems. Be as specific as possible in defining the interface and integration requirements. Incomplete definitions result in costly system modifications. Will the PPCs interface with the department CAD, NCIC, state and local systems, arrest and booking, crime analysis, etc.?
Define General System Requirements

- Open systems architecture provides hardware and software platforms that promote the use of standards. By adhering to these standards your applications are independent of a specific vendor and you can obtain the most competitive system.

- Graphical user interface (GUI), a term that has become almost synonymous with “user friendly,” provides menus, buttons, icons and other easily recognizable screen images. GUI is easier for users to learn and operate.

- Built-in editing and error checking requires the system to have built-in tables and menus so that incorrect information is rejected before it is input into the database. The system is easier to use since pull-down tables and menus are available to the user.

- Context sensitive help allows users to open help notes as they are using various applications.

- Flexible communication design allows the system to interface with a variety of external and internal systems so that it can easily integrate into the agency’s communications environment.

- Prototyping capability creates a version of some or all of the capabilities of the final system. Although its function is usually limited, it allows the user to “see” how the system will operate and provides for the first stage of system modifications to occur.

- Define the number of units, communication links, and networks that are required for the system to perform and provide capability to those personnel who will be users. The vendor can scale his system, but make sure that you define the minimum number of acceptable units.

- Define the environmental conditions of your application of PPCs. How, or will, the units be mounted in a patrol vehicle? What are the space, temperature and humidity limitations? What are the requirements for ruggedness, battery life, communications, and storage? What are the variations in available light that define the readability of the display? These are primary restrictive requirements of the PPCs and will result in a minimal number of viable systems for procurement.

Training Considerations

Training is a vital requirement for all new system procurement. Adequate training time and documentation must be provided by the the agency.

Various alternatives should be considered as they affect the costs. You may wish to contract with a vendor to provide basic PC training to your agency. You should consider a program of “Train the Trainer” vs. vendor-provided training for all staff. Who will provide user and maintenance training? How extensive is the training? Are the costs included in the budget and proposal? How much time is required for training? What is the learning curve? Will
training be provided on or off site? Is online interactive training available? These questions should be addressed in order to determine the startup period for the new system and the availability of staff during the training cycle.

**Documentation**
Documentation is another critical requirement of a new system. Two major types of documentation should be obtained: 1) user and training manuals, and 2) system design documentation.

User manuals provide the basic document for system usage and are the essential documents for training. System documentation contains all the design details and in some cases may contain the program “source code.” Ownership of the source code will be an issue in any contract; however, you must attempt to obtain the source code, particularly for highly customized systems and for designs from new or small companies. Ownership of this code is the only protection you may have if your vendor has future problems, i.e., bankruptcy, purchase by another company.

Other issues to be addressed are the ease of use and understandability of the documentation, frequency of updating, and number of copies available.

**System Security**
System security is another vital concern for law enforcement executives. Any system that is purchased should provide for several levels of security. Of particular concern are systems that allow general access to personnel files, criminal files, investigation reports, and other sensitive data. In addition, dialup access requires further levels of security to prevent “hacking” into confidential files. Extreme care must be exercised in the area of data access to ensure that all critical data are not compromised. You must define your specific security environment and requirements.

**Vendor Concerns**
The vendor requires honesty and detail in your specifications, just as you require the same from them. Vendors want to participate in procurements that have clearly defined requirements and expectations. They want to provide a bid that ensures that you receive the best value that they can give for the funds available. Vendors must provide the customer with sufficient information to select the most advantageous product that the customer can receive. If bid responses do not include this, then reject them.

Strive for mutual understanding and partnership from the beginning. Define the agency management team and project manager so that the vendor will be dealing with a single representative from your agency. You might share the evaluation criteria with your bidders so that you can receive a proposal that emphasizes, and more specifically the agency needs. Establish realistic schedules and milestones for the project. Dealing with vendors requires an
agency to develop realistic expectations of performance and system costs. Are you willing to pay for higher quality components or staff? Are you willing to bear the costs of maintenance and support? Sharing some of the following with your bidders may help to yield systems that will better meet your specifications.

- What are the criteria for system performance and acceptance?
- Are you considering all vendor responses equally? Is there a level playing field?
- What are the shortcomings of the existing system? What limitations exists on new system implementation?
- What progress reporting requirements are there?
- What will be the organizational relationship between the vendor and the customer?
- What are your budgetary constraints? Sometimes vendors can offer alternative means of funding system acquisition such as leasing or deferred payment. Are there restrictions against this that are placed by city charter or local officials?

**Other General Considerations**
Implementing a new means of crime reporting, using computer technology will be a complex undertaking. The following are a few common problems and suggestions on how to avoid them.

- Schedules are difficult to predict and cutover, conversion, data collection, and training are frequently underestimated. Increasing your estimates by 50 percent might be appropriate.
- Technical expectations can be difficult to manage. The conflict, between a proven stable technical solution and one that is state of the art, is real. Further, agencies must decide if the benefits of implementing technology are worth the risk.
- Build a partnership with your vendor. You will be working together for many years and it is important that you develop a good working relationship.
- Contract issues are also critical. If it is not in the contract, then it does not exist. If you really need performance bonds, liquidated damages, and other assurances, then be prepared to pay for it. Specify the details of the design as clearly as possible. Leave little to interpretation and include the vendors response to the RFP as part of the contract.

Reproduced with permission from the IACP Law Enforcement Information Management Section.  
http://www.IACPtechnology.org
Backup Systems

by Sonina Matteo

Mobile data computers’ introduction to police patrol is comparable to the takeover of digital cameras in the film camera industry. The wide variety of laptops, notebooks and PDAs used on patrol, is mind boggling for those of us who were taught to write everything on a 3x5 pocket pad. The uses of this technology include CAD, report-writing, wanted and motor vehicle checks, instant messaging, RMS and many others. Frequently, in-car printers turn out traffic and parking citations, copies of reports and photos. Reports are transmitted wirelessly and instantly downloaded into the RMS. When all this technology is working, the results are vast improvements to work levels from just a few years ago. When the technology is not working “Houston, We Have a Problem” is a fitting portrayal.

Like it or not, the further we push to get better, cheaper, and faster technology, the more dependent we are on its use, and, the harder it is to look back at where we came from. Unfortunately, systems and equipment do go down and as hurricanes Katrina and Rita have taught us, we may need to be prepared for more that just a minor interruption. As for our officers and civilians, the “old timers,” may be able to revert to the “old ways,” but what about our newer employees? Many of the latest hires do not have experience in preparing or handling paper reports or manually completing an arrest. Some agencies use of silent dispatch is so extensive that new officers lack radio skills.

For these reasons, as we build data systems, redundancy and back-up is required. From extra keyboards and wiring, to backup servers and spare phone-lines, this investment may keep a patrol car or the entire mobile data computer system operational.

By the way, hold onto a few of those paper reports, ticket books, pens and 3x5 pads. Maybe, put them near the flashlights. Also, an occasional drill on the use of manual reporting and radio usage will be helpful.

Captain Robert Liberati
Prince George’s County Police Department—Maryland

Data Backup for A Law Enforcement Mobile Data Solution

Laptop computers which link to a law-enforcement agency’s computer network through radio frequency technology will provide an officer with computer access to, among other things, the dispatch system, to department-maintained databases, and to the FCIC/NCIC
network. In addition these computers can serve as a mobile office for report writing, electronic mail, and other office functions.

According to senior systems engineers for police departments the reliance on mobile laptops and other wireless handhelds, as well as the growing crime prevention databases, has driven up the demand to ensure that system backups are reliable and accurate. Departments need a secure and efficient solution that would safeguard crucial information. Backups can be done on the road or from a central in-building location.

The purpose of this brief is to address the ways that police officers can perform data backup on the road. Several backup strategies can meet the various demands of mobile law enforcement environments. Solutions depend on the type of systems or end-user equipment currently in use. Enterprises can supply police officers with removable storage devices, provide access to external hard disks, or synchronize data between mobile data terminals or laptops and file servers, and even allow scheduled incremental backups from the road.

**Removable Storage**

Some of the peripherals being used in police cars include radio modems, GPS/AVL units, magnetic stripe readers, computer controller light bars, bar code scanners, ticket printers, and TV camera inputs. This list of possible devices far exceeds the limited number of interrupts (card slots) available on laptops. This is why removable storage products (plug-and-play devices with bundled software) are a viable solution for mobile police officers.

- **USB Drives**—Universal Serial Bus (USB) shares interrupts thus limiting the need for several extra ports. A removable storage unit for mobile workers that allows them to backup data is the Universal Serial Bus (USB) Drive. USB Flash Drives are small, lightweight, removable and rewritable data storage devices that today supports from 4 to about 64 GBs and are used for general storage and transfer of data between computers.

- **Microdrives**—Microdrives are also an option. Microdrives are like miniature hard disks that can be used to backup data and supports upwards of 6+Gibibytes (GiBs). They can fit into the Compact Flash (CF) Type II slot of a portable computing device.

Either the USB or Microdrive solution can put gigabytes of data in a small form-factor device that fits into a pocket. Most of these removable storage solutions on the market today have a synchronization feature.

**Enterprise Class Backup and Synchronization Solution**

If you prefer to back up and synchronize data rather than just back up files then there are enterprise class backup and synchronization solutions.
With a growing number of police departments the mobile laptops or handhelds are being utilized like a desktop computer on the road. This presents two challenges to IT managers in police departments: protecting critical data that resides on police officer’s mobile data terminals or on their laptops; and providing access to network-stored data to these mobile officers who may be frequently offline. There are products on the market that solve these issues and enables mobile police officers to be as productive on the road as they are at police headquarters, while protecting their local data.

When laptop users are disconnected from the network, an enterprise class backup and synchronization solution can work in the background to present the user with virtualized, cached data from selected network file servers, displaying the same folders and drive mappings as if the user were connected to the network. When laptop users reconnect to the enterprise network, that technology solution contacts a synchronization server that resides on the appliance, and synchronizes user file changes with what is stored on the network file server. Additionally, new local data on the laptop can be backed up over the mobile network. All data transfer is typically optimized for the WAN and incorporates advanced compression techniques to reduce synchronization time and bandwidth.

These solutions can perform highly efficient laptop data backup, identifying in seconds what files have been updated and then leveraging WAN–efficient compression techniques to synchronize files—even if the files are open and in use. In short this type of appliance and software solution enables both data protection and access for the roaming mobile data user if the mobile data unit (or laptop) is damaged or has an operating system or software failure locally. Recovery involves synchronizing the new laptop with the files stored on the network fileserver.

By using this solution rather than dedicated file servers in the remote office and with specialized software on individual laptops, police clients are backing up their remote data in real-time over the WAN. These products can replicate the network structure of an enterprise onto user laptops, creating a virtual network wherein the same mapped drives, network names, hierarchies, links, and shortcuts are available in a disconnected/unplugged state. The solution should work over your wireless network (whether digital cellular, municipal/city wireless, or Wi-Fi), dial-up, VPN, and LAN connections.

When looking for ways to make sure that there is data backup being done effectively on mobile data terminals there is a need to look beyond just that requirement. Public Safety administrators or police chiefs should look at software which enables centralized data management and protection for laptops and desktops, and cached, virtual access to network file server content when offline, with no changes required to mapped drives or folders.

Developed for IACP’s Technology Desk Reference, 2006 by Sonina Matteo, Tech Research Services
http://www.techresearchservices.com
Training

Source: Illinois State Police, IT Command

No mobile computing system will be successful unless those who use it are fully trained. Agencies may be inclined to purchase less training support than is needed, on the assumption that power users will train others, but this approach has the potential for severe implementation problems that will never be fixed.

Training needs and objectives should be identified early in the project and a complete training plan developed that ensures all potential users are trained to the level that they require for the system to be useful. Some agencies have taken to including refresher training in the purchase agreement, ensuring that the software provider will return a number of months after implementation to maintain training levels. Some companies have introduced web-based training as a means to fulfill follow-up training needs.

Line managers and supervisors must be fully committed to getting their staff trained, and must support the training plan and schedule.

Classroom Training

While essentially providing the best quality of training for computer technology, classroom training to the actual users lends itself to many drawbacks, particularly to a large agency.

• Cost of bringing officers to the site, travel and hotel reimbursements for some. Difficulty coordinating multi-shift enforcement responsibilities and scheduling officers for training.
• Challenge of training officers with different learning curves and various knowledge levels of the users in one room.
• Technologically challenged users may either hold up an entire classroom, or will be left behind, making the time just a waste.
• It would be prudent to have several trainers to assist users with computer problems.
• Timeliness of computer training with receipt of computers is essential.
• If classroom training is provided well in advance of the equipment, there will be little retention.
• The training site will need to have ample power outlets and additionally wireless access inside the room will be necessary.
With smaller agencies where travel to a site is minimal or where class sizes are smaller, classroom training is very advantageous.

**Support Group Training**

Consider providing the user base with the minimum of technical skills needed, but provide a core group of individuals with more advanced skills. These users can become the first line support group and should receive advanced technical training on equipment and technology being deployed. Your users support group in the field may include the following:

- **Work Group Mobile Data Coordinator**—Primary contact for support and the individual through whom problems are escalated to the Mobile Computer Team.
- **Mobile Computer Team**—This group should be secondary support and should mostly be dealing with coordinators reporting issues. Technical skills of this group would include knowledge of computer hardware, software, operating systems, and databases.
- **Telecommunicator**—Call taker or telecommunicator who could evaluate criminal history hits or assist with other inquiry interpretations.
- **Vehicle Technician**—Individual knowledgeable of the in-vehicle installation and the various interoperability issues of radios and mobile computers.

**Vendor Provided Training**

The vendors providing the software and hardware for your mobile data system could be utilized as a training resource. Not only can the vendor assist with cost of training implementation, they have other resources in terms of experts in the field, presentation materials, etc. which can provide better quality and more thorough training to your groups.

- Consider including in any of your mobile data vendor contract, a clause which requires them to provide at no charge, semi-annual classroom training at a central location to be decided by the agency. Vendors also may offset some costs of providing training by development training manuals or providing a training facility.
- Include in your RFP or RFI a request for the vendor to explain how they would be able to provide training on their product. They may offer on-line training, electronic manuals, CDs, or may even propose sending trainers to various work sites.
- Consider your vendors as part of your deployment team, keeping them informed of how your agency is progressing in its planning and implementation. This provides more ownership to the vendor. When it comes time to providing training, the vendor is more attuned to the specific needs of your users.
Computer Based Training (CBT)
Since this training can be loaded on the mobile computer, it provides officers with the opportunity to utilize the actual computer equipment they will be assigned to take the training. CBT can be developed in-house and can offer many benefits:

- Cost effective to deploy
- Training can be changed when new technology is deployed
- Officers can take the training at the time of equipment assignment and then use the equipment and its software to reinforce training
- Officers can advance at their own pace
- Training can be easily worked into an officer’s work day with little impact on agency productivity
- Officers will retain the training on their mobile computer for reference at a later date, if needed

Intranet Site
Depending on the technology, many mobile environments will permit users to access an Intranet site. This affords an agency many opportunities for providing essential information to the user, including the following training tools:

- How-to files
- FAQs
- Tips and shortcuts
- Successful user of mobile technology by fellow officers
- Download of small files and updates
- Contact numbers for assistance

On-Going Training
Keep your support group up-to-speed on changing technology by providing centralized classroom training. During the initial implementation, every six months would be recommended. After implementation, consider providing an annual training session. The support group, particularly the coordinators, will benefit from advanced technical training. The Mobile Data Team will benefit from face-to-face discussions on what is happening in the field and the ability to discuss issues or problems they are encountering.

Post-Implementation Evaluation
You cannot set it and forget it. Follow-up with your users after implementation regarding problems or issues they are having. Identify outstanding training needs and then develop methods of filling these holes either by sending files, messages, intranet, handouts, etc. Complex training needs of small groups may require remedial training provided by the IWN coordinator.
Reference Materials
Not many officers will take time to read large documents. Some of the following have proven to be beneficial:

Reference Card
Consider a small laminated two-sided card for quick reference concerning inquiries or hot keys for the computer and/or software.

Initial Instructions
A single sheet of paper can be inserted inside a mobile computer to “Welcome” the new user to their device. Initial instructions might include:

• How to power the computer on
• How to access and log onto the client application
• Where to find additional information
• How to power down the computer
• Who to call for help

Mobile Computer Desktop
Help files and tutorials can be placed on the mobile computer. To assist the officer in accessing these files quickly, place shortcuts on the computer desktops with easy to reference file names. You could require that the training presentations of all the vendors be provided electronically and these placed on the desktop for user reference.

Reproduced with permission from Illinois State Police, IT Command, 2006. Further reproduction without express written permission is strictly prohibited.
http://www.isp.state.il.us/
Sample Policy
Source: IACP Technology Clearinghouse

This policy is included in the TDR as an example of procedural guidance for Mobile Computing efforts. As law enforcement executives tailor this policy to their specific agencies, the policy will need to be redrafted in the context of existing local ordinances, provisions of union contracts and all other state and federal laws. Departments must ensure that all other related policies are updated to be consistent with the provisions of this new policy.

Every effort has been made by the IACP Research Center Directorate and the Technology Technical Assistance Program (TTAP) to ensure that this policy incorporates the most current information and contemporary professional judgment on the issue. However, law enforcement administrators should be cautious that no “model” policy can meet the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decision, and collective bargaining agreements, and each agency needs to tailor its policies to ensure compliance with all laws, regulations and agreements.

Police Department—General Order
Policy Statement
1. Purpose—This order provides standards and guidelines for the proper and authorized use of the mobile data computer (MDC) by department members as a means of communicating with dispatch and other members, and maintaining the status of field units.

2. Definitions—A mobile data terminal is a mobile communication device that provides for communication with the computer aided dispatch (CAD) system and field units, between field units, or between fixed terminal locations.

3. Authorized Users—No member of the department will use an MCT unless they have received the following training:
   a. mobile data computer terminal certification
   b. mobile data computer terminal orientation

4. All authorized personnel are provided with, and should have available, a copy of the Mobile Data Computer Terminal—Quick Reference Guide. This guide
provides detailed information on all of the specific functions and recommended operations of these units. (Disposition codes and self initiated codes are included in this form.)

Proper Use

1. **Priority Calls**—All calls will be sent through the MCT when a member has an MCT available. The following guidelines apply to the dispatching of calls:
   a. Priority One and Priority Two calls will be dispatched via MCT and by voice over the radio.
   b. Priority Three and below calls will normally be dispatched via MCT only.

2. **Safe Vehicle Operation**—When operating a vehicle, the safe operation of the vehicle is a member’s primary responsibility. Use of the MCT is always of secondary importance, and the member should consider the need to safely stop the vehicle before using the MCT if the use is going to divert the member’s attention from the safe operation of the vehicle.

3. **DMV/CCH Checks**—The MCT will be used for Department of Motor Vehicle (DMV) and Computerized Criminal History (CCH) and wanted checks when a member has an MCT available, unless the member is out of the vehicle, or the use of the MCT cannot be done safely.

4. **Use For Official Business Only**—All communications between or among field or fixed units are permitted for official business only. MCT communications may be monitored and are a matter of public record.

5. **Status Changes**—Other than traffic stops, unit status changes will be accomplished via MCT, (subject to Section A4 above) i.e. clearing from calls or self initiated activities, going enroute to calls, etc. All members must update their status as soon as possible and practical except that:
   a. Officers will go in-service, out-of-service, and will acknowledge Priority One and Priority Two calls by voice and MCT.
   b. Tactical information will be relayed via voice communication.

6. **Traffic Stops**—Traffic stops will be initiated by voice radio communication and may be cleared by voice or MCT at the member’s discretion.

7. **Other Uses**—If time and circumstances permit, and the MCT can be used safely, self initiated activities, follow up, meal and coffee breaks and field contacts will be communicated via the MCT.

8. **LEDS Information**—Members shall not release any Law Enforcement Data System (LEDS) activated information obtained via the MCT to the public that is subject to the LEDS Agreement and is not subject to public disclosure. Any requests of this nature should be referred to the Police Records Unit.

9. **Car to Car MCT Use**—Car to car communication via the MCT is permitted, subject to the same restrictions as those between field units and dispatch.
10. Confirming Wants—Any wanted person or vehicle information received via MCT must be confirmed through dispatch or Police Records.

Improper Use of the MCT
1. Professionalism—All communications via the MCT will be professional and conducted in a business like manner.

2. Prohibited Comments—The transmittal of any sexist, racist, vulgar, derogatory or discriminatory messages is specifically prohibited.

3. Modifications to Equipment—No member, unless specifically authorized to do so by the department, will make any modification to the MCT, the vehicle MCT set-up, or to the MCT software, except for the user defined options such as screen intensity.
   a. Supervisor Responsibility—Supervisors will monitor MCT messages to review call response and work load, and to ensure MCT use conforms to department standards.
   b. Responder Safety—No portion of this General Order is intended to prohibit or limit the member from making safety conscious decisions. If there is a comprise of safety in a particular situation related to the use of the MCT, the member is expected to use voice communications.

4. In any police vehicle in which a mobile data computer terminal is installed, there will be no smoking or other use of tobacco products. Extreme care should be exercised when consuming beverages near the terminal. Spill-resistant or leak-proof containers are recommended.

5. Officers should refrain from having the Communications Center personnel FAX anything to the Department, in regards to data run on the MDC terminals by the officers. The officers have the ability to print the data at a remote printer at the Department, or have the Community Service Officer (CSO) run any requested data. Warrant verifications are done by our department personnel. In extreme emergency situations, the Center can confirm an out of area warrant, but they cannot cancel one entered by our department Community Service Officers. These cases are extremely rare.

Operational Procedures and Duties
1. Log on/Log off—Each officer assigned a patrol unit equipped with MDC communications shall log on to the system using his/her squad number and call sign. When the unit is staffed with two officers, the officer that is operating the radio should be logged on as the primary officer on the terminal.

2. Use of the Report Number Function—Officers should retrieve their report numbers from their terminals whenever possible. An exception to this may be
when an officer is away from his terminal and needs the report number to complete certain reports (ie. domestic abuse, etc.). Only the primary officer can generate the report number by terminal. Just type RN and transmit.

3. **Use of Disposition Codes**—Disposition codes should be entered by the officers whenever possible. Type in CU.Disposition code (ie: R, NR, CIT, WARN, etc.) This does not mean that officers won’t go back in service on the radio; it just means that they will clear out the call themselves and let everyone know via radio that they are back in service. See the quick reference guide for disposition codes.

4. **Use of Enroute/Arrival/Available Function Buttons**—Officers should use the function buttons whenever possible. Only backup officers assigned to the calls can use the available function. The primary officer needs to provide the disposition code prior to clearing. The arrival button should be used by everyone with a functioning terminal. This is used to eliminate a dispatch step. This should not take the place of the voice transmission of arriving on scene. This is an officer safety issue, and voice transmission should occur as well.

5. **Use of Self-Initiated Codes**—Self-initiated codes are used with the On-Scene function key. These should be used whenever possible. Some of the self initiated codes (e.g., disorderly conduct or family problem) appear to be inappropriate for self initiation by an officer. These types of calls were set up for non in-progress follow-up type situations. Any in-progress type situations should be initiated by the dispatcher, via the officer radio transmission. See the Quick Reference Guide for the authorized self-initiated codes.

6. **Accident Disposition Code**—This code is used specifically by our agency. Since we do not generate accident report numbers in the field, this allows the officer to indicate that a report was left, with no number being generated.

7. **General Use**—Officers are encouraged to run as much data as possible on the terminals. This is particularly true when running of 10-27, 10-28, and 10-29’s. In situations where officers are involved in the investigation of disabled vehicles, minor accident investigation, abandoned suspicious vehicle complaints, or self-initiated follow-up contacts, the officers should run related data on the computer. Officers are encouraged to utilize all of the capabilities of the MDC, provided no specific officer safety concerns can be articulated in these types of situations.

8. **Traffic Stops**—During traffic stops, investigation of occupied suspicious vehicles, and other in-progress situations where there is more evident officer safety concerns, officers should always check out with the dispatcher prior to the contact. The officers should provide license plate numbers and other pertinent
data during this initial transmission. During these types of incidents, it is more appropriate for the officers to have the dispatcher run any related data, unless the officer is comfortable in running this data on the MDC terminal.

**Dispatch Center**
1. The Dispatch Center terminal shall remain logged on to the system at all times.

**Area and System Messages**
1. Area-wide (police department) and system-wide (county-wide) administrative messages may only be sent for official department-orientated purposes. System-wide broadcasts should contain information which should be distributed to more than one department. System-wide messages are generally sent out via the telecommunicators in the Bolo/atl files.

**Monitoring of Transmissions**
1. Monitoring of MDC transmissions may be periodically and randomly conducted by the Chief of Police or his designee to insure compliance with Department General Orders and Procedures. All MDC terminal transmissions are subject to open records requests.

A policy courtesy of the IACP Technology Technical Assistance Program—October 2006

Adapted from policies available at the IACP Technology Clearinghouse.
http://www.IACPtechnology.org
Sample Press Release

This press release is included in the TDR as an example for communicating with the media about a new technology project. As law enforcement executives tailor this press release to their specific agencies, it will need to be redrafted in the context of local collaborations, project status and timelines. Departments must ensure that all information in the press release is accurate.

This media contact may be the only opportunity that agencies have to introduce the public to a department’s technology efforts, and follow-up reports of malfunctioning technology may be difficult to manage. Thus, prior to releasing a statement to the media about a new technology deployment, it is essential that technology be tested repeatedly for usability.

Every effort has been made by the IACP Research Center Directorate and the Technology Technical Assistance Program to ensure that this press release incorporates the general issues related to in-car cameras. However, law enforcement administrators should be cautious that no “sample” press release can meet the needs of any given law enforcement agency. Each agency must to tailor its media relations to ensure compliance with all laws, regulations and agreements.

NEWS FOR IMMEDIATE RELEASE | January 1, 2010

Jane Banker Gets Computer Funds for Anytown Police Department
Police Chief Paul Smith and Congresswoman Jane Banker announce funds providing all patrol officers and detectives with mobile computer terminals in their police cars

Washington, DC – Adding to her long-time record of supporting local law enforcement, Congresswoman Jane Banker secured half of a million dollars of federal funding for the Anytown Police Department’s Mobile Computing Terminal Project (MCT). Paul Smith today announced the funding with Anytown Police Chief Paul Smith.

“As we move into the 21st century, today’s police officers need more than just handcuffs and weapons to be effective. They need quick access to information,” said Banker. “This money will help give the Anytown Police Department the technological tools necessary to prevent crime and, just as important, devote critical time and effort towards community policing.”
The $500,000 will help fund the department’s goal of providing all patrol officers and detectives with mobile computer terminals linked to local, regional and state law enforcement systems. This project has been under way for several years. The city has dedicated a combination of Federal Crime Act grant funds and local funding totaling $26 million.

“Ms. Banker has gone to bat for this department repeatedly,” said Chief Paul Smith. “She has come through again to enhance our expansion of essential technology. We are extremely grateful.”

This year’s appropriations will go will help the Anytown Police Department purchase desktop and laptops computers for detectives, modems and dock stations for patrol cars, and investigative case programming.

“New computer technology has played a major role in maximizing officer efficiency,” said Banker. “However, without federal funding assistance, the technology necessary for maximum efficiency and effectiveness is out of reach.”

The money was designated in the Commerce, Justice and State Department Appropriations legislation passed by the House of Representatives last year.

A press release courtesy of the IACP Technology Technical Assistance Program—October 2006
Additional Resources

Technology today has become a critical component in every law enforcement agency’s arsenal against crime. It is imperative that all law enforcement agencies have at their disposal the latest technology to not only solve crime but also to be used as a force multiplier in an era of shrinking personnel resources. It is important for every law enforcement executive to maximize both their awareness of technology and where to find technology resources. As we all know, technology is expensive and it is often time-consuming to ascertain which is the best technology for a specific application within a law enforcement agency. To make this task easier, the following approaches are suggested:

- The chief law enforcement executive should be committed to staying current on technology issues
- Develop and maintain a working partnership with the International Association of Chiefs of Police, a leader in developing and implementing technology
- Maintain an awareness of the role of the federal government with law enforcement technology, especially the National Law Enforcement and Corrections Technology Centers, and use them as a research and development program
- Refine the ability to learn from others successes as well as failures

Technology today is often the difference between solving a current or cold criminal case, saving a life and protecting our officers from harm. An agency executive who fails to bring modern technology into their law enforcement agency is truly doing a disservice to the agency, the officers, and the community. It is the intention of this publication to assist the law enforcement executive with this exact task, to utilize technology to make our communities safer, our officers safer, prevent and solve crime.

Chief Paul Schultz
Lafayette Police Department—Colorado
IACP Technology Clearinghouse—Serves as a one-stop shop for technology related information that addresses all aspects of public safety from line personnel to senior executives.

http://www.iacptechnology.org

National Law Enforcement and Corrections Technology Center—Created in 1994 as a component of the National Institute of Justice’s (NIJ’S) Office of Science and Technology, NLECTC system serves as an “honest broker” offering support, research findings, and technological expertise to help State and local law enforcement and corrections personnel perform their duties more safely and efficiently.

http://www.justnet.org

SEARCH—The National Consortium for Justice Information and Statistics, is a nonprofit membership organization by and for the states. SEARCH’s primary objective is to identify and help solve the information management problems of state and local justice agencies confronted with the need to exchange information with other local agencies, state agencies, agencies in other states, or with the federal government.

http://www.search.org

Wireless LAN Association—The WLANA is a non-profit educational trade association, comprised of the thought leaders and technology innovators in the local area wireless technology industry.

http://www.wlana.org

Search Mobile Computing.com—The guide to the TechTarget network of industry-specific IT Web sites.

http://www.searchmobilecomputing.com
Mobile Computing Glossary

A

Amber Alert—Broadcast message.

Automatic Vehicle Location (AVL) Systems—Computer-based vehicle tracking system.

B

Backup—The activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe.

Battery—An electrochemical cell (or enclosed and protected material) that can be charged electrically to provide a static potential for power or released electrical charge when needed.

Benchmark—A point of reference by which something can be measured.

BOLO (Be on the Lookout)—Broadcast message.

Boot—To load an operating system into the computer’s main memory or random access memory (RAM). Once the operating system is loaded (and, for example, on a PC, you see the initial Windows or Mac desktop screen), it’s ready for users to run applications.

Broadband—A wide band of frequencies is available to transmit information.

Browser—An application program that provides a way to look at and interact with all the information on the World Wide Web.

Bus—In computer architecture, a bus is a subsystem that transfers data or power between computer components inside a computer or between computers and typically is controlled by device driver software.

Byte—Is a unit of data that is eight binary digits long.
C

Cache—A place to store something temporarily.

CAD (Computer Aided Dispatch) Systems—Allows dispatchers to create events in the computer as they are received from citizens calling the Communications Center as well as from deputies over the radio.

Computer—A computer is a device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed.

CPU (Central Processing Unit)—Processor unit of a sequential computer system.

D

Data Terminal—Computer transmit and receive equipment, including a wide variety of dumb terminals (terminals without embedded intelligence) in the form of programmed logic. Most data terminals provide a user interface to a more capable host computer, such as a mainframe or midrange computer.

Decryption—Decryption is the decoding and unscrambling of received encrypted data. The same device, host computer or front-end processor, usually performs both encryption and decryption.

DMA (Direct Memory Access)—Allows devices on a bus to access memory without requiring intervention by the CPU.

DRAM (Dynamic RAM)—Memory which periodically needs refreshing, and is therefore usually slower than SRAM but is cheaper to produce.

G

GUI (Graphical User Interface)—Graphical (rather than purely textual) user interface to a computer.
Hardware—The physical aspect of computers, telecommunications, and other devices. Includes not only the computer proper but also the cables, connectors, power supply units, and peripheral devices such as the keyboard, mouse, audio speakers, and printers.

Hot Spot (or Hotspot)—Wireless LAN (local area network) node that provides Internet connection and virtual private network (VPN) access from a given location.

(HPC) Handheld PC—The term adopted by Microsoft and its supporters to describe handheld computers employing Microsoft’s Windows CE operating system.

Laptop Computer—Usually called a notebook computer by manufacturers, is a battery- or AC-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently.

MIMO (Multiple Input, Multiple Output)—An antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver).

Mobile IPv6 (MIPv6)—A protocol developed as a subset of Internet Protocol version 6 (IPv6) to support mobile connections.

Mobile wireless—The use of wireless devices or systems aboard motorized, moving vehicles

Mouse—A small device that a computer user pushes across a desk surface in order to point to a place on a display screen and to select one or more actions to take from that position.

Notebook Computer—A battery or AC powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces.
PCS (Personal Communications Service)—A new, lower powered, higher-frequency competitive technology to cellular. Whereas cellular typically operates in the 800-900 MHz range, PCS operates in the 1.5 to 1.8 GHz range. The idea with PCS is that the phones are cheaper, have less range, and are digital. The cells are smaller and closer together, and airtime is cheaper.

PDA (Personal Digital Assistant)—Any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy.

Pen-Based Computers—Mobile computers that provide handwriting recognition as input to the units.

Peripheral—Generally refers to any external device attached to a computer, such as a mouse, keyboard, printer, any USB device, etc. The term is used to indicate that the device is external to the PC case.

Pocket PC—The term adopted by Microsoft and its supporters to describe handheld computers employing Microsoft’s Pocket PC operating system.

Portable Wireless—The operation of autonomous, battery-powered wireless devices or systems outside the office, home, or vehicle; examples include handheld cell phones and PCS units.

PSU (Power Supply Unit)—The component that provides power for a computer to function.

RAM (Random Access Memory)—Computer memory which can be written to and read from in any order.

ROM (Read Only Memory)—Computer memory which cannot be written to during normal operation.
**S**

**Software**—General term for the various kinds of programs used to operate computers and related devices.

**T**

**Touchpad**—A device for pointing (controlling input positioning) on a computer display screen. It is an alternative to the mouse.

**U**

**USB (Universal Serial Bus)**—Plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers).

**V**

**Voice Based Computers**—Mobile computers that provide voice recognition and translation for input to the units.

**W**

**Wi-Fi**—A wireless data networking protocol generally used connect PCs and laptops to a network. Also know as 802.11b and WLAN(Wireless LAN), it is the most common means of wireless networking and operates at 2.4 GHz.

**Wireless**—Telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.

**WLAN (Wireless Local Area Network)**—A wireless LAN is a data communications system providing wireless peer-to-peer (PC-to-PC, PC-to-hub, or printer-to-hub) and point-to-point (LAN-to-LAN) connectivity within a building or campus. In place of TP or coaxial
wires or optical fiber as used in a conventional LAN, WLANs transmit and receive data over electromagnetic waves. WLANs perform traditional network communications functions such as file transfer, peripheral sharing, e-mail, and database access as well as augmenting wired LANs. WLANs must include NICs (adapters) and access points (in-building bridges), and for campus communications building-to-building (LAN-LAN) bridges.

**WPAN (Wireless Personal Area Network)**—A personal area network, a network for interconnecting devices centered around an individual person's workspace, in which the connections are wireless.