



IMPLEMENTING A MOBILE COMPUTING SYSTEM

AN ITI WHITEPAPER ON
MOBILE TECHNOLOGY FOR
PUBLIC SAFETY

IMPLEMENTING A MOBILE COMPUTING SYSTEM

An ITI Whitepaper on Mobile Technology for Public Safety

INTRODUCTION

Mobile computing is here to stay. Today, agencies of almost any size are able to implement a mobile computing system, thus keeping their most valuable resources, their officers, on the streets where they are needed.

With mobile computing, a patrol vehicle literally becomes a rolling office, complete with NCIC inquiries, report writing, mug shot and line-up viewing and a host of related activities. Mobile computing completes the toolset required for Community Oriented Policing to take foothold and thrive. Unfortunately, there are many pitfalls awaiting the novice implementer of a mobile computing system. This document is intended to address these pitfalls and to provide a plan for successfully implementing a mobile computing system for your agency.

Many agencies indicate that they want to have mobile computers. Unfortunately, not all are ready to unleash mobile computers on their patrol officers. Many years ago it was taught that computer automation was of no value when applied to a process that was not well defined. In other words, if there isn't a good manual process, it can not be automated. In a slightly different fashion, this holds true of mobile computing applications within the public safety industry. Agencies that have not yet implemented computer automation internally, are not ready to implement mobile computing. Thus, if your agency is still writing reports by hand, it is probably not best for your first automation project to include mobile computing.

Similarly, agencies which have purchased public safety software, but have not fully utilized the functionality, either through a lack of effort with configuration and setup, or through inadequate training, should not look to mobile computing as a means to resuscitate their automation dreams.

Mobile computing is best applied as the final phase of a comprehensive automation project. This project should include the following phases, prior to mobile computing:

- Computer Aided Dispatch (if applicable)
- NCIC Interface
- Records Management
- Custom Reporting

By fully and successfully implementing each of the above project phases, an agency can be properly prepared to finally take the step of moving their "system" to the patrol vehicles.

TYPES OF MOBILE COMPUTING SYSTEMS

Over the years, there have been a number of types of mobile computing systems. The earliest systems consisted of one to four line screens in proprietary terminals that were linked to the station based system via RF networks. Modern systems consist of either ruggedized or consumer-grade laptops connected across the Internet, with or without a Virtual Private Network (VPN) via a TCP/IP based commercial wireless network.

Proprietary networks have become a poor choice in almost any area that has a substantial cellular network. As cellular networks have evolved to carry wireless data, the cost for using these networks has become significantly less expensive. At the same time, bandwidth, or the amount of data that can be transferred in a given period of time, has increased substantially. Later, under “Wireless Service Selection” we will discuss the differences between carriers and explain the options in more detail. Suffice to say that in any area where there is a modern cellular system, it would be a poor choice to build a proprietary system. Due to competition, wireless carriers continue to expand their networks and increase bandwidth. When you own your own system, you are responsible for enhancing as well as maintaining it. Thus, you can usually purchase service on a commercial system for less money than you would spend to keep a proprietary system maintained and up-to-date.

Another area to consider when discussing types of mobile computing systems is form factor. In addition to laptop PCs, everything from two-way pagers and cell phones to wireless PDAs can be utilized in a mobile computing environment. Although less functional, these solutions are certainly less expensive, and can be utilized to address specific needs. One such example is ticket writing, a recent addition to the wireless offering of many vendors. Using PDAs and portable printers, ticket writing systems can automate a once mundane activity and eliminate after-the-fact data entry and errors.

Finally, when considering types of mobile computing systems, you should consider whether your system will serve only your agency, or include others. This could include other agencies for which you dispatch, as well as county wide or area wide systems which allow officers from multiple jurisdictions to interact and share information through their mobile computers. Systems of this type are usually tied to a specific vendor, but will not be constrained in the future. You should consider your needs and how your agency works as the starting point when shopping for a mobile computing system.

PLANNING YOUR MOBILE COMPUTING SYSTEM

Once you have determined that your agency is both ready for and committed to mobile computing, it's time to plan. Obviously money is the key factor here, so start gathering all that you can, because it's going to be expensive.

To obtain money, either from your state, county or city leaders, or through grants, you need to have justification. Any more, it's almost credible to simply say that “everyone else has them”. But there is some rather rudimentary data that can be used to help justify the expense. This can include the following:

- A list of the total calls for service your agency has handled over the past three years. It's usually good to show this as a ratio to the total number of officers you had during each year. In most cases, you will find that your number of calls for service has increased, and the number of calls per officer has also increased. It's easy to draw the conclusion that as your calls for service

continue to increase (it's the national trend), you will need to add officers. Adding technology can increase productivity and allow your existing staff to handle more calls for service.

- If your agency dispatches for itself, look at the number of calls for service per dispatcher during the past several years. Again, this ratio in most cases has increased, and again you can show that as this trend increases, you will have to add dispatchers and dispatch facilities. Mobile computing can reduce the reliance on dispatchers for relaying all information to the officers on the street.
- The total number of arrests made by your agency each year, for the past three or more years. You will probably find that this number has increased as well. Document the amount of time, on average; it takes for an officer to process a prisoner. Since much of this can be accomplished from the mobile computer, with the officer back on the street after dropping off the prisoner, you can again show higher productivity.
- Look at the total number of overtime hours during the past year, three years or even five years. Has this continued to rise? If so, perhaps your officers are using time after their shift to complete reports that could be done, in full or in part, during their shifts, via mobile computing.
- On average, how many times does a patrol officer return to the station during a shift? With mobile computing, you can significantly reduce this trend. With the exception of prisoner processing, officers with mobile computers can remain on the street during most of their shift.

In almost all cases, it's best to develop a justification based on statistics for installing a mobile computing system. This same analysis will also help you understand the tasks that are most important for you to automate with your mobile computing project.

Once the justification is complete, you can look for grant money. Mobile computing was the single largest benefactor of COPS MORE grants in the late 90's and early 2000's. Today, with grants shifting to Homeland Security, the most important factor seems to be multi-jurisdiction systems. Thus, if your mobile computing system also ties to a jurisdictional or regional data sharing system, you have a leg up on other agencies vying for grant monies.

Now it's time to get down to business. What most project leaders do next is search for the right laptop. Wrong! The laptop computer should be the last item that you select. You first have to find out your wireless service options, and select software that will meet your needs. Then your hardware selection can be made based upon the requirements of the wireless system and the selected software. There will be plenty of time to shop for laptops later in your project, and since computer hardware changes continually, it's in your best interest to wait.

WIRELESS SERVICE SELECTION

As discussed above, you need to find out which commercial wireless vendors have wireless data service available within your venue. The key players, along with contact information are:

AT&T Wireless (877) 882-5256
<http://www.wireless.att.com/cell-phone-service/welcome/index.jsp>

Sprint/Nextel (800) 211-4727
<http://www.sprint.com/index.html>

T-Mobile USA, Inc.
<http://www.tmobile.com/>

(800) 937-8997

Verizon Wireless
(Joint venture of Verizon Communications and Vodafone)
<http://www.verizonwireless.com/b2c/index.jsp>

(800) 922-0204

Each of these companies, along with smaller regional cellular carriers, provide wireless data services. However, their services vary and new technology is literally coming out every year. Thus, it's somewhat of a minefield, and there is no one set of criteria by which to objectively compare these vendors. What follows, is information of which to be aware, and ideas for determining which vendor is best for your project.

All of the above carriers provide TCP/IP based Internet access on their wireless data networks. Don't be wary because this involves an Internet connection. Using Virtual Private Networks (VPNs), intelligent routing and firewalls, you can safely utilize the Internet to transmit your wireless data. Also, virtually no carrier or software vendor sends the information in plain text. Through the use of data compression, data encryption and proprietary formats, mobile data systems for public safety are quite safe.

Transmission speeds, bandwidth and all terms used for claiming how fast a vendors network is are all based on theoretical values. In other words, they are little white lies. Coverage maps also are usually wishful thinking at best and propaganda at worst. How then do you determine which vendor really has the best service for your venue? Try these approaches:

- Offer to sign a Non Disclosure Agreement (NDA) in order to see the vendors engineering drawings showing their actual coverage. All vendors have these, and some will produce them.
- Insist on being provided one or more demo systems (modems) which you then utilize in a patrol vehicle to test actual coverage throughout your venue.
- Most wireless services can be judged by your experience with their voice service. This is true especially where you are using digital voice service. The same towers are utilized along with the same network. Thus, if you have experienced poor voice service with Vendor A's system, you will probably recognize the same poor service with their wireless data.
- Check with other agencies within your area who are using mobile computing. So many agencies are now utilizing mobile computing systems that there is a wealth of information available from others whose bruises have had time to heal.

No matter which (or all) of the above techniques you use, do your homework. Never take the vendors word for coverage, equipment or price. The communications industry has one of the highest turnovers of any industry in the United States. That should tell you plenty.

If you already have a software vendor, be sure and check that their software is supported on the wireless network that you are considering. This is an important step that has been missed in the past. Although incompatibilities are rare when using TCP/IP, not all systems play well together. Your software vendor may have information that can save you time and money.

It is not a good idea to lock in to a long-term contract. This is simply because the industry is evolving and thus new and improved services are coming out at a rapid pace. If you are locked into a long-term contract, you may find yourself paying too much and unable to utilize a better alternative.

Since you don't want to be locked long-term into any one technology or vendor, it usually doesn't make sense to purchase some of the higher cost mobile modems. The benefits of these units are that they are located in the trunk where they will be less likely to be abused, they have higher power and they can include global positioning. All of this is true. However, you can usually do very well with a PC/MCIA modem card (laptop card that slides into a slot) with an external antenna and a separate GPS receiver that connects to your laptop. In all, you will save as much as \$ 800 per vehicle, and with less invested, be freer to switch wireless carriers in the future. And don't forget, the wireless vendors will usually throw in some or all of the cost of the lower priced cards.

One final thought on wireless cards. Stay away from the ones that have an on-board battery. These are nothing but trouble. For best results, select a wireless card that obtains its power directly from the PC.

Finally, signing a contract with a wireless carrier should be the last item on your project. All carriers can get your wireless service activated and hardware in your hands within a couple of days. There is plenty of time to do this while you wait for mobile computers and software installation. Besides, you don't want to pay for wireless service that you are not ready to use.

SOFTWARE SELECTION

As discussed earlier, there will continue to be a strong inkling to go shop for mobile computing hardware. Don't do it. The next step (which can be done in concert with selecting your wireless service) is to determine what software you will be using.

Mobile computing is obviously a hot topic, and as such there are a host of vendors involved. All will be happy to take your money, and I assure you that once it becomes known that you have a pending project, they will come out of the woodwork. There are some issues however that separates the vendors:

- Determine if the mobile computing software being offered was developed entirely by your in-house software vendor. Many software vendors either utilize third party software entirely, or embed third party communications software in their mobile computing offerings. This becomes very important when software enhancements, updates or bug fixes are considered. With more than one vendor involved, there can often be delays or other difficulties involved.
- Find out all of the hardware, operating system software and related items that will be needed to support the vendor's software. In many cases, vendors require you to purchase specific hardware (often from them) to act as a Message Switch for your mobile computing system. Less restrictive vendors allow you to select the hardware based on requirements they provide.
- Find out what type of data compression and data encryption is being used by your vendor. Reference the National Institute of Standards and Technology (NIST) website for information on their Advanced Encryption Standard (AES). This information is available at their Computer Security Resource Center. <http://csrc.nist.gov/csrc/fedstandards.html>
- Determine how software on the mobile computers will be updated. Present technology allows for updates to be downloaded directly from the server, without technical assistance. Systems

that require a visit to each patrol vehicle with a CD-ROM should now be considered old. This one step can save you many hours of work down the road.

- Is the system web-browser based (considered a “thin client”), or executable-based (considered a “thick client”)? There are pros and cons to both types, and you should consider the ramifications of each. In general, thin client applications maintain all software (and thus changes) on the server, and are considered easier to maintain. However, thick client applications are much more flexible and can provide disconnected use. Your choice will depend mainly on the features that you are looking for.

HARDWARE SELECTION

Ok, now you’re ready to look at hardware. You basically have two choices, consumer-grade or hardened, also known as ruggedized. There is no one right answer that fits every situation. Consumer grade laptops will always have the latest specifications (faster, more RAM, larger hard disks, etc.), and will cost less than a ruggedized unit. Since ruggedized units are proprietary, and sell far fewer units than a consumer grade laptop, they cost more and are based on older technology. This is simply due to the fact that with proprietary design, it is impossible to keep up with the consumer market, as well as the fact that a manufacturers return on investment takes longer. Where you may spend \$ 1,500 on a consumer grade laptop, a ruggedized laptop can set you back as much as \$ 6,000. Obviously you need to plan on using this unit for three to five years to recognize your investment. Unfortunately, this means that you will have the same technology for three to five years.

Regardless of what a manufacturer tells you, don’t count on being able to upgrade ruggedized laptops. With the exception of perhaps adding some RAM, it simply is not likely to happen. As hardware changes (processors, memory type, etc.) their newer designs almost always require major modifications. This means that new technology cannot usually be incorporated into the hardware that you bought one, two, three or more years ago. This should not scare you away from buying a ruggedized laptop. Just don’t believe that it is going to be able to be upgraded substantially in the future.

Very few laptops and their mounting systems meet federal airbag deployment guidelines. In general, only those that mount the screen on the dashboard and stow the electronics elsewhere are able to meet these guidelines. Unfortunately, these same units usually are not portable at all, and taking them out of a patrol vehicle means de-installing. One of your first considerations should be whether or not your officers should (need to) take the laptop out of the patrol vehicle. Departments that have take home vehicles, or those where officers need to work outside of their cars for extended periods of time (in a sub-station, etc.) may have needs to allow their officers to take the laptop computers in and out of the patrol vehicle. If this is the case, you should look at a laptop with a docking station. The docking station allows you to quickly install or remove the laptop without dealing with wiring and connectors. Your department can get a waiver that allows you to deactivate the right seat airbag.

There are bound to be agencies in fairly close proximity to yours who have mobile computers. Visit them and see what hardware they purchased, how it is installed and how it is serving them. You will need to take into consideration how their agency has their vehicles setup, and their mission. A highway patrol officer who generally does traffic patrol all day has different needs than a county or municipal officer who is answering calls for service. After visiting other agencies and looking at literature, ask for on-site demonstrations. Choose the top three (or so) laptops and ask for a field trial unit from each vendor. The small amount of money you spend installing and de-installing the units is insignificant

when compared to making a bad decision. Some of the things your “evaluation” officers should consider when trying out the field trial units are as follows:

- Position of the computer. Were you able to mount or install it in a satisfactory position?
- Feel of the keyboard
- Readability of the screen in all conditions (daytime, nighttime, etc.)
- Quality of the sound. Most mobile computing software utilizes sound alerts.
- Durability. If you have problems with the field-trial, what do you think will happen when you install a number of these same units?
- Backlighting of the keyboard. This is a popular feature that you will only find on ruggedized units.
- Brightness control on the display. This also is a popular feature that you will only find on ruggedized units. Some vendor’s software will also go into a “night” mode, where softer colors are used.
- Availability of a magnetic card reader. Many state’s drivers licenses are being made with embedded magnetic cards. Whether magnetic cards continue to be used or some newer technology such as Radio Frequency ID’s (RFID) is adopted, there will be a need for some form of identification reader. If the unit you select does not have a magnetic card reader, ensure that it has an available serial or USB port for a peripheral unit to be attached if necessary.

INSTALLATION CONSIDERATIONS

Any wireless modem will perform better with an external antenna. Most PC/MCIA card modems allow for this. If you are using a trunk mounted modem, you will have to use an external antenna. This involves installing a glass mount, magnetic or trunk lid mount antenna and running the cabling to the modem. For the minimal cost involved, this will add considerably to the wireless experience.

Don’t forget to consider access to other important equipment such as your shotgun, flashlight charger, etc. We have seen installations where the mobile computer hardware blocked access to the shotgun, and new shotgun mounts had to be purchased. It’s best to think this out and try the installation on one vehicle before ordering equipment for all of your vehicles.

If your fleet has special purpose vehicles such as SUV’s or vans that will be equipped with mobile computers, you will need to consider how these systems will be mounted. The mounting will most likely need to be different than your regular patrol vehicles.

Power is always a consideration. If you are using a ruggedized computer, it probably came with a 12 VDC power system that can be wired directly into an auxiliary fuse. Most consumer grade laptops run off of 117 VAC, and will require either a special adapter for 12 VDC from the manufacturer, or the use of an inverter. An inverter converts 12 VDC to 117 VAC. Some less expensive inverters can generate electronic noise that may interfere with your two-way radio or other equipment. In addition, there are power management devices available that will monitor the mobile computer and shut it off after a pre-determined time if the computer is left on while the vehicle is shut off. This can help ensure that you don’t find patrol vehicles with dead batteries when you go to start them.

It's best to utilize a qualified installer who has experience with mobile computers. Such an installer can properly mount the computer and peripheral equipment and deal with power. Modems and software are best installed by qualified representatives of the respective vendors.

PUTTING IT ALL TOGETHER – MAKING YOUR PROJECT SUCCESSFUL

We hope that we haven't scared you away from mobile computing. Without a doubt, there is work to do in order to implement a mobile computing system. However the rewards are enormous. Let's not forget though the very most important final step necessary to ensure a successful project; training. Training your staff so that they can properly and effectively utilize mobile computers is the key to success.

Training should not only cover operation and use of the mobile computer, but should cover the Dos and Don'ts associated with maintenance of the unit. We often see units that are uniquely setup in each patrol vehicle. Just as users would do at home, they have downloaded screen savers, wallpaper, mouse pointers and such to an agencies mobile computer. In some cases, these attempts at personalizing a computer have led to infestation by viruses. An analogy that we have used is this: Would you allow an individual officer to modify the action of their department issued weapon? Certainly not, and in almost all cases there would be immediate disciplinary action. Why then do so many agencies look the other way as individual officers "personalize" department computers, and in the process create problems? We suggest that as part of your mobile computing project you adopt a strict policy of leaving all system "configuration" to the system administrator(s).

If properly planned, executed and maintained, a mobile computing system can make your agency significantly more productive and professional. While the costs are significant, it is much less expensive than hiring, training and outfitting additional officers. With budget constraints as they are, more and more agencies will need to turn to mobile computing for help in meeting the growing demand for police services.

THE FUTURE - THE ROLE OF MOBILE COMPUTING IN INVESTIGATIONS

Most agencies think of mobile computing as a tool for patrol officers. As public safety software evolves, and more and more information become quickly accessible from a mobile computer, investigators can increasingly utilize this technology as well. Whether using a mobile computer or a wireless PDA, inquiries into NCIC and department databases can be valuable tools for the investigator on the street.

In most cases, investigators are able to make use of consumer grade laptop computers. Equipped with mobile software and a PC/MCIA modem card, these small tools can be carried to the station, in the vehicle or inside buildings, wherever an investigation leads. Without the expense of ruggedized computers and mounting solutions, arming your investigators with mobile computers can be an especially rewarding investment.

ABOUT ITI

Information Technologies, Inc. (ITI) is a leading provider of public safety software throughout the United States. ITI was founded in 1988 and serves over 500 public safety agencies in 43 states and the U.S. territories. ITI has been involved in the development and support of public safety software and mobile computing solutions for over ten years.

About the author: Neil Kurlander is a thirty-five year police veteran serving the last fifteen as chief of police. If you would like additional information concerning the use of technology to address the issue of racial profiling at (800) 814-4843 or by e-mail at sales@itiusa.com.