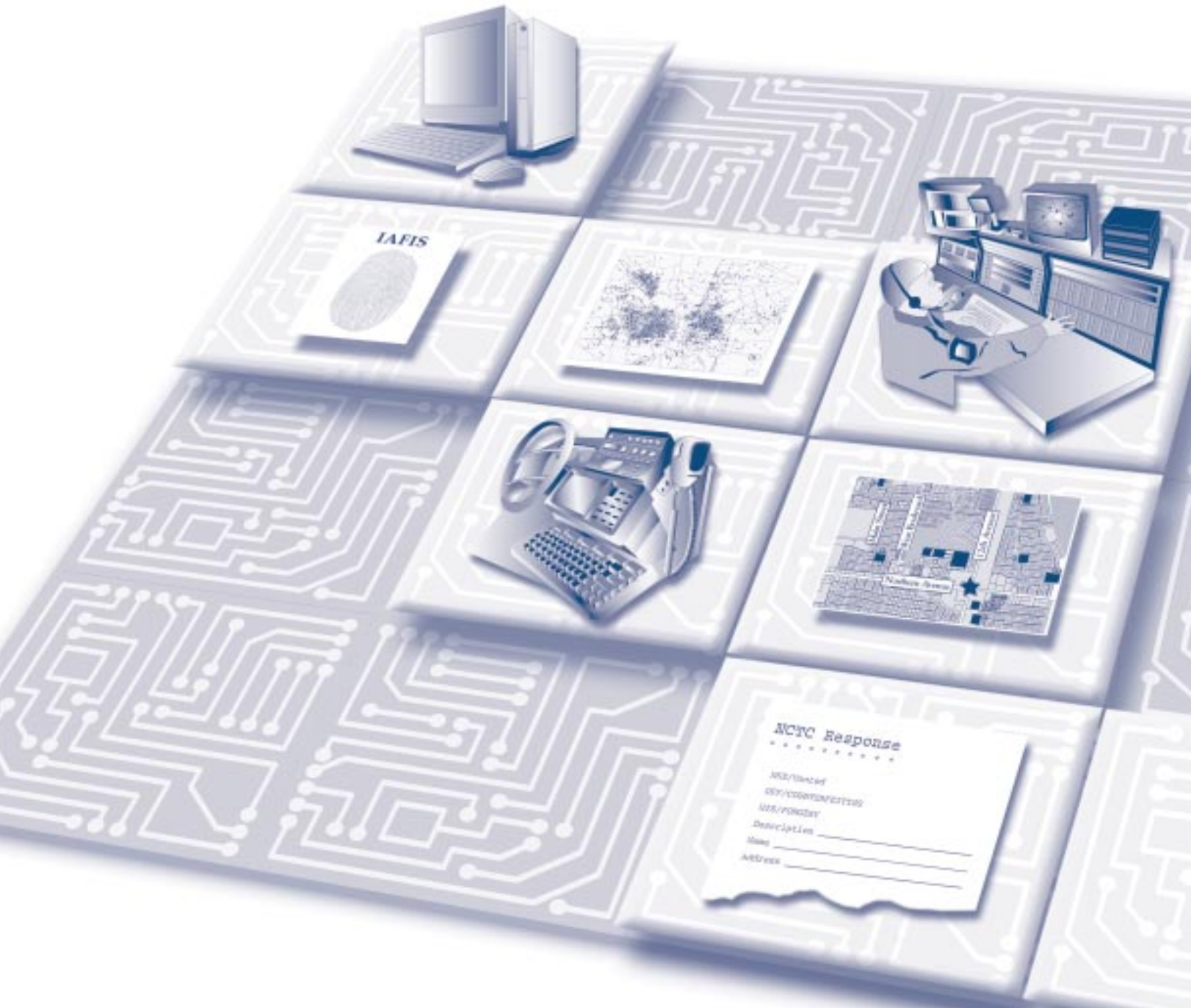
National Law Enforcement and Corrections Technology Center

A Guide for Applying Information Technology in Law Enforcement

National Law Enforcement and Corrections Technology Center



U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

A Guide for Applying Information Technology in Law Enforcement

March 2001
NCJ 185934

Office of Science and Technology

David G. Boyd
Director

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #96–MU–MU–K011 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

Preface

The information revolution of the past two decades has resulted in more people having faster access to more accurate data than ever before. Both the public and law enforcement practitioners expect agency information systems to respond quickly with an enhanced ability to recognize crime patterns and problem areas. As a result, law enforcement agencies need to improve their information systems to better analyze and use the data they collect.

This guide is intended to help law enforcement practitioners plan and implement information system upgrades and address connectivity and data sharing issues. It is intended to be a primer rather than a definitive treatise on the subject. The authors' goal is to help public safety agencies integrate such public safety information systems as computer-aided dispatch, records management, geographical information systems, and mobile computing. Using the principles outlined in this guide, law enforcement professionals can choose the technologies that best suit their needs and incorporate them into their day-to-day operations.

Acknowledgments

This document represents a collaboration among the centers within the National Law Enforcement and Corrections Technology Center (NLECTC) system. The following individuals contributed their time, expertise, and experience to the development of this document.

NLECTC–Southeast

Project Management
William R. Deck

Primary Writer/Editor
Maura Maness

Law Enforcement Applications
Pat Matysek

Information Systems and Security
Vance Stone

NLECTC–Northeast

Wireless and Mobile Computing Systems
Sal DiRaimo

Mobile Computing
James Morelli

NLECTC–Rocky Mountain

Geographic Information System and Crime Mapping
Noah Fritz

NLECTC–West

Implementing Information Technology
Mike Epstein

Border Research and Technology Center

Concept Development
Chris Aldridge

We would also like to thank Maj. Coleman Knight (Ret.) of the Mount Pleasant, South Carolina, Police Department for reviewing this document for accuracy and application.

Table of Contents

About the National Institute of Justice

The National Institute of Justice (NIJ), a component of the Office of Justice Programs, is the research agency of the U.S. Department of Justice. Created by the Omnibus Crime Control and Safe Streets Act of 1968, as amended, NIJ is authorized to support research, evaluation, and demonstration programs, development of technology, and both national and international information dissemination. Specific mandates of the Act direct NIJ to:

- Sponsor special projects and research and development programs that will improve and strengthen the criminal justice system and reduce or prevent crime.
- Conduct national demonstration projects that employ innovative or promising approaches for improving criminal justice.
- Develop new technologies to fight crime and improve criminal justice.
- Evaluate the effectiveness of criminal justice programs and identify programs that promise to be successful if continued or repeated.
- Recommend actions that can be taken by Federal, State, and local governments as well as by private organizations to improve criminal justice.
- Carry out research on criminal behavior.
- Develop new methods of crime prevention and reduction of crime and delinquency.

In recent years, NIJ has greatly expanded its initiatives, the result of the Violent Crime Control and Law Enforcement Act of 1994 (the Crime Act), partnerships with other Federal agencies and private foundations, advances in technology, and a new international focus. Examples of these new initiatives include:

- Exploring key issues in community policing, violence against women, violence within the family, sentencing reforms, and specialized courts such as drug courts.
- Developing dual-use technologies to support national defense and local law enforcement needs.
- Establishing four regional National Law Enforcement and Corrections Technology Centers (NLECTC), a Border Research and Technology Center, and three special offices to join the National Center in Rockville, Maryland, to form the NLECTC system.
- Strengthening NIJ's links with the international community through participation in the United Nations network of criminological institutes, the U.N. Criminal Justice Information Network, and the NIJ International Center.
- Improving the online capability of NIJ's criminal justice information clearinghouse.
- Establishing the ADAM (Arrestee Drug Abuse Monitoring) program—formerly the Drug Use Forecasting (DUF) program—to increase the number of drug-testing sites and study drug-related crime.

The Institute Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the Department of Justice, and the needs of the criminal justice field. The Institute actively solicits the views of criminal justice professionals and researchers in the continuing search for answers that inform public policymaking in crime and justice.

About the Law Enforcement and Corrections Standards and Testing Program

The Law Enforcement and Corrections Standards and Testing Program is sponsored by the Office of Science and Technology of the National Institute of Justice (NIJ), U.S. Department of Justice. The program responds to the mandate of the Justice System Improvement Act of 1979, which directed NIJ to encourage research and development to improve the criminal justice system and to disseminate the results to Federal, State, and local agencies.

The Law Enforcement and Corrections Standards and Testing Program is an applied research effort that determines the technological needs of justice system agencies, sets minimum performance standards for specific devices, tests commercially available equipment against those standards, and disseminates the standards and the test results to criminal justice agencies nationwide and internationally.

The program operates through the following:

- The **Law Enforcement and Corrections Technology Advisory Council** (LECTAC), consisting of nationally recognized criminal justice practitioners from Federal, State, and local agencies, assesses technological needs and sets priorities for research programs and items to be evaluated and tested.
- The **Office of Law Enforcement Standards** (OLES) at the National Institute of Standards and Technology develops voluntary national performance standards for compliance testing to ensure that individual items of equipment are suitable for use by criminal justice agencies. The equipment standards developed by OLES are based upon laboratory evaluation of commercially available products in order to devise precise test methods that can be universally applied by any qualified testing laboratory and to establish minimum performance requirements for each attribute of a piece of equipment that is essential to how it functions. OLES-developed standards can serve as design criteria for manufacturers or as the basis for equipment evaluation. The application of the standards, which are highly technical in nature, is augmented through the publication of equipment performance reports and user guides. Individual jurisdictions may use the standards in their own laboratories to test equipment, have equipment tested on their behalf using the standards, or cite the standards in procurement specifications.
- The **National Law Enforcement and Corrections Technology Center** (NLECTC), operated by a grantee, supervises a national compliance testing program conducted by independent laboratories. The standards developed by OLES serve as performance benchmarks against which commercial equipment is measured. The facilities, personnel, and testing capabilities of the independent laboratories are evaluated by OLES prior to testing each item of equipment. In addition, OLES helps NLECTC staff review and analyze data. Test results are published in consumer product reports designed to help justice system procurement officials make informed purchasing decisions.

Publications are available at no charge through NLECTC. Some documents are also available online through the Justice Technology Information Network (JUSTNET), the center's Internet/World Wide Web site. To request a document or additional information, call 800–248–2742 or 301–519–5060, or write:

National Law Enforcement and Corrections Technology Center
P.O. Box 1160
Rockville, MD 20849–1160
E-mail: *asknlectc@nlectc.org*
World Wide Web address: *http://www.nlectc.org*

About the National Law Enforcement and Corrections Technology Center System

The National Law Enforcement and Corrections Technology Center (NLECTC) system exists to support the Nation's structure of State and local law enforcement and corrections. The United States has more than 18,000 law enforcement agencies, 50 State correctional systems, and thousands of prisons and jails. The fragmented nature of law enforcement and corrections impedes the dissemination of valuable new information, fosters a patchwork marketplace that discourages the commercialization of new technologies, and underscores the need for uniform performance standards for equipment and technologies.

The National Institute of Justice's (NIJ's) Office of Science and Technology (OS&T) created NLECTC in 1994 as a national system of technology centers that are clearinghouses of information and sources of technology assistance and that also attend to special needs, including technology commercialization and standards development.

The NLECTC system's purpose is to determine the needs of the law enforcement and corrections communities and assist them in understanding, using, and benefitting from new and existing technologies that, increasingly, are vital levers of progress in criminal justice. It is especially important to note that NIJ/OS&T and the NLECTC system are the only current programs developed by the Federal Government that focus solely on the development and transfer of technologies to State and local law enforcement and corrections.

NLECTC is a program of NIJ, the research and development arm of the U.S. Department of Justice. The system currently consists of a national center, four regional centers, and three speciality centers. Also contributing to the initiatives of the center system is the Office of Law Enforcement Standards. The centers are colocated with a host organization or agency that specializes in one or more areas of technology research and development.

The National Center, located in Rockville, Maryland, is the system's information hub. Regional centers are currently located in California, Colorado, New York, and South Carolina. Speciality centers located around the country deal with border matters (California), commercialization of law enforcement and corrections technologies (West Virginia), and forensic science (Florida).

Each center shares roles with the other centers and has distinctive characteristics. All are focused on helping law enforcement and corrections take full advantage of technology's rapidly growing capacity to serve the purposes of crime control and the criminal justice system.

A national body of criminal justice professionals, the Law Enforcement and Corrections Technology Advisory Council (LECTAC), helps identify research and development priorities, thereby influencing the work of the NLECTC system. In addition, each NLECTC center has a regional advisory council of law enforcement and corrections officials. Together, LECTAC and the advisory councils help to keep the NLECTC system attentive to technological priorities and the needs of law enforcement and corrections. They help to link the end user with the developer to create technologies that adequately meet operational requirements and establish which potential technologies should be pursued for development.

All of the current regional centers have distinctive roles or focus areas, that, in many cases, are aligned with the expertise of host organizations and agencies. The centers are currently operated under cooperative agreements or interagency agreements with host

organizations and agencies whose employees staff the centers.

To receive more information or to add your name to the NLECTC mailing list, call 800–248–2742 or 301–519–5060, or write:

National Law Enforcement and Corrections Technology Center
P.O. Box 1160
Rockville, MD 20849–1160
E-mail: asknlectc@nlectc.org
World Wide Web address: *http://www.nlectc.org*

The following is a list of NLECTC regional and affiliated facilities that assist NIJ in fulfilling its mission.

NLECTC–Northeast
26 Electronic Parkway
Rome, NY 13441–4514
(p) 888–338–0584
(f) 315–330–4315
E-mail: *nlectc_ne@rl.af.mil*

NLECTC–Southeast
5300 International Boulevard
North Charleston, SC 29418
(p) 800–292–4385
(f) 843–760–4611
E-mail: *nlectc-se@nlectc-se.org*

NLECTC–Rocky Mountain
2050 East Iliff Avenue
Denver, CO 80208
(p) 800–416–8086
(f) 303–871–2500
E-mail: *nlectc@du.edu*

NLECTC–West
c/o The Aerospace Corporation
2350 East El Segundo Boulevard
El Segundo, CA 90245–4691
(p) 888–548–1618
(f) 310–336–2227
E-mail: *nlectc@law-west.org*

Border Research and Technology Center
1010 Second Avenue, Suite 1920
San Diego, CA 92101–4912
(p) 888–656–2782
(f) 888–660–2782
E-mail: *brtcchrisa@aol.com*

Office of Law Enforcement Standards
100 Bureau Drive, Stop 8102
Gaithersburg, MD 20899–8102
(p) 301–975–2757
(f) 301–948–0978
E-mail: *oles@nist.gov*

Office of Law Enforcement Technology Commercialization
Wheeling Jesuit University
316 Washington Avenue
Wheeling, WV 26003
(p) 888–306–5382
(f) 304–243–2131
E-mail: *oletc@nttc.edu*

National Center for Forensic Science
University of Central Florida
P.O. Box 162367
Orlando, FL 32816–2367
(p) 407–823–6469
(f) 407–823–3162
E-mail: *natlctr@mail.ucf.edu*

About the Office of Law Enforcement Standards

The Office of Law Enforcement Standards (OLES) was established as a matrix management organization in 1971 through a Memorandum of Understanding between the U.S. Departments of Justice and Commerce based upon the recommendations of the President's Commission on Crime. OLES' mission is to apply science and technology to the needs of the criminal justice community, including law enforcement, corrections, forensic science, and the fire service. While its major objective is to develop minimum performance standards, which are promulgated as voluntary national standards, OLES also undertakes studies leading to the publication of technical reports and user guides.

The areas of research investigated by OLES include clothing, communication systems, emergency equipment, investigative aids, protective equipment, security systems, vehicles, weapons, and analytical techniques and standard reference materials used by the forensic science community. The composition of OLES' projects varies depending upon priorities of the criminal justice community at any given time and, as necessary, draws upon the resources of the National Institute of Standards and Technology.

OLES assists law enforcement and criminal justice agencies in acquiring, on a cost-effective basis, the high-quality resources they need to do their jobs. To accomplish this, OLES:

- Develops methods for testing equipment performance and examining evidentiary materials.
- Develops standards for equipment and operating procedures.
- Develops standard reference materials.
- Performs other scientific and engineering research as required.

Since the program began in 1971, OLES has coordinated the development of nearly 200 standards, user guides, and advisory reports. Topics range from performance parameters of police patrol vehicles, to performance reports on various speed-measuring devices, to soft body armor testing, to analytical procedures for developing DNA profiles.

The application of technology to enhance the efficiency and effectiveness of the criminal justice community continues to increase. The proper adoption of the products resulting from emerging technologies and the assessment of equipment performance, systems, methodologies, etc., used by criminal justice practitioners constitute critical issues having safety and legal ramifications. The consequences of inadequate equipment performance or inadequate test methods can range from inconvenient to catastrophic. In addition, these deficiencies can adversely affect the general population when they increase public safety costs, preclude arrest, or result in evidence found to be inadmissible in court.

Chapter 1. Introduction

Today, law enforcement agencies have more technologies available to them than ever before (computer-aided dispatch/records management system (CAD/RMS) software, mobile computing, and digital radios, to name a few. With so many options available, the questions about what information technology (IT) solutions are right for an agency can be overwhelming, especially in times of tight resources and budgets.

This document is a product of the National Law Enforcement and Corrections Technology Center system, a program of the U.S. Department of Justice, National Institute of Justice, Office of Science and Technology. This guide is intended help law enforcement agencies in their efforts to develop and/or enhance their information systems.

Think of the many ways technology could improve your agency. Here are a few examples to get you started:

- A combined search of local, State, and Federal criminal histories, available by entering a single request from a computer in a patrol vehicle, thus reducing radio traffic.
- A database then can be queried, resulting in more reliable crime analysis reporting or investigative searches.
- A system that can link persons, addresses, property, and vehicles, thus reducing data entry and improving safety to the officer in the patrol vehicle.
- Technology allowing officers to enter incident reports, supplementals, and field checks into the central database from the patrol vehicle, thus providing more timely agencywide access to data.
- Online documentation or guidance for entering reports and classifying crimes, policies, and regulations, thus providing quick clarification and reducing re-entering of information.
- Electronically signing onto a system via a laptop at the beginning of shifts, thus improving accountability of resources.
- Dispatched messages sent silently to a patrol vehicle, thus improving chances of stopping crimes in process and protecting the officer.

This guide offers the law enforcement community a description of what information system technologies are currently available and information to help you determine how to incorporate them into your agency's day-to-day business. It also explains the functions technology solutions provide, shows how they can be integrated, and provides you with key considerations in developing an implementation plan and a procurement strategy. The guide is not intended to offer indepth technical discussions, nor will it talk about specific manufacturers or their products.

Why a Guide?

This guide was developed as a result of National Law Enforcement and Corrections Technology Center (NLECTC) assistance visits made to several law enforcement agencies of various sizes across the Nation. It became apparent during these visits that most agencies needed access to similar information and that these agencies could use a "roadmap" to implement information technology. The concept of a guide was born out of this need.

Purpose and Scope

First, this is a guide. It is not a panacea. Like all guides, this one provides a place to start and tips on what to do along your journey to help organize your efforts. There are many decisions that will need to be made by you, your agency, or the people you hire to help you in your project.

Information technology is a world of its own, and so is law enforcement. Marrying the two can result in a more efficient and, hopefully, safer working environment and community. Regardless of where technology is used, the activities in your agency's day-to-day business can be characterized as a business process. Applying information technology is not (and should not be) simply automating a process. It is using technology where it makes sense and brings about greater efficiencies.

This guide is organized around the key components of an information technology project plan, specifically, application software, network/hardware, and mobile data computing. We also provide pointers on developing a Request for Proposal (RFP) and evaluating the responses.

We have concentrated on several types of information technologies for law enforcement, including RMS, CAD, geographic information systems (GIS), crime mapping systems, and mobile computing. These were chosen as necessary building blocks of sound law enforcement operations. Of course, there are many other elements, such as the Integrated Automated Fingerprint Identification System (IAFIS), National Incident-Based Reporting System (NIBRS), and digital photographic files. These applications also are critical to law enforcement, but will require a more detailed analysis than this document is designed to provide.

As you work through an information technology project, you may want to have a dictionary of computer terms, which you can find in the computer/Internet section of most bookstores. One particularly thorough book is the *Dictionary of Computer and Internet Terms,* published by Barron's Educational Series, Inc. You can also find resources on the Internet (e.g., the www.whatis.com Web site).

Below is a short description of each of the following eight chapters:

Chapter 2. Planning an Information Technology Project. A review of project planning steps as they apply to an information technology project, including the crucial step of conducting the Information Technology Assessment *to establish* your needs.

Chapter 3. Conducting an Information Technology Assessment. An indepth review of the technology assessment process, providing an explanation of the necessary steps and basic procedures for conducting/participating in the assessment.

Chapter 4. Law Enforcement Information Systems: A Look at Application Software, Part I. An indepth review of application software systems used by law enforcement. The first of three components of an IT project.

Chapter 5. Law Enforcement Application Systems: A Look at Application Software, Part II. An overview of two emerging technology solutions—geographic information systems and crime mapping.

Chapter 6. Information System Connectivity. A review of hardware and connectivity needs in layman's terms. The second component of an IT project.

Chapter 7. Mobile Data Communications. The third component of the IT project. This review of mobile data computing introduces the equipment needed to implement such a system, as well as the considerations for choosing which type of communication is the best for your agency.

Chapter 8. Request for Proposal Development and System Selection. Step-by-step pointers for developing and issuing of the RFP and then conducting a fair, comprehensive evaluation of the responses.

Chapter 9. Installation Management and Beyond. A review of how your agency can prepare for implementation and how to work with vendors to get the most out of the system for the lifetime of the product.

Chapter 2. Planning an Information Technology Project

Planning an information technology project follows many of the same steps you may have used to plan other projects (establish objectives, identify resources, determine needs, explore options, select the optimal alternative, and implement the solution. The real challenge comes when you try to accomplish these tasks. Since most of us are end users of technology and not developers of technology, the start of an IT project sends us into another world, with a whole new vernacular. This chapter details project planning steps *as they apply to IT projects*. An IT system acquisition can be as simple as the purchase of commercially available, off-the-shelf items that easily fit together with very little effort or risk, or the procurement of a complex system composed of many subsystems, requiring an experienced, dedicated effort to ensure success.

By proceeding through the following series of steps, you can plan a project that leads to a successful procurement and installation (steps 10 through 12 are discussed later in this guide):

Step 1. Establish the Scope of the Project Based on Your Agency's Goals and Objectives

Step 2. Get Help

Step 3. Form a Working Group

Step 4. Educate Your Team

Step 5. Conduct an Information Technology Assessment

Step 6. Develop Overall System Needs

Step 7. Develop a System Design and Schedule

Step 8. Develop a Cost Estimate

Step 9. Obtain Management Approval

Step 10. Develop and Issue Request for Proposal (if necessary)

Step 11. Select System

Step 12. Implement System and Monitor Performance

Step 1. Establish the Scope of the Project Based on Your Agency's Goals and Objectives

The first step is to establish the scope of the project. The assignment might be as ill defined as "modernize the IT systems in our agency" or as specific as "upgrade our RMS, move all the records to this new system, and make sure it works with other systems such as CAD." Now is the time to define the scope, but it must be within the bounds of your agency's vision, goals, objectives, and price range.

Prior to undertaking a major IT project, the agency's long-range goals and objectives should be reviewed. If these do not include contemporary technology objectives, they may need to be refined. Examples of long-range goals are: improved information sharing, reliable field report writing systems, and reliable field interfaces with National Crime Information Center (NCIC) checks and local database searches.

Internal and external management are the primary source for the agency's long-range plans, including funding opportunities. Therefore, it is important to identify the cost and performance expectations of the managers and to communicate these back once they are documented. This task may not be an easy one, but defining system expectations will help educate and prepare management for the system, personnel, and financial impacts. Managers also should identify end users by group and job type. Although individual end users may not be identified, a valid cross-section of the end-user community should be provided. For example, patrol officers, dispatchers, and emergency services are valid user groups that could be represented.

Another point to bear in mind is that the new system may provide capabilities far beyond the current system and may force operational changes to properly use this new technology. The scope of change that

the organization is able to tolerate must be considered. It is important to ensure that expectations, change tolerance, and technology are clearly understood by all stakeholders.

Step 2. Get Help

Regardless of the system to be acquired, if its purchase, installation, and operation are outside your capabilities, get some help. Help can be as simple as a quick look from someone knowledgeable with the system or as complicated as hiring a full-time employee, consultant, or company to help run the process. The adage, "You get what you pay for," rings true here. The 16-year-old technical genius who lives next door was a great resource when your computer game crashed on your home PC, but do you really want to rely on his advice for your agency's networking issues?

Actions further along in the process, particularly steps 5 and 6, require technical skill sets that are probably not present in your agency's staff. A data analyst, business analyst, and network engineer will be responsible for creating a snapshot of how your agency processes information and how these processes can be improved *using technology.* If these personnel do not exist within the agency, they should be hired to perform the assessment. It is essential that the business analyst be objective, which may not be possible when inhouse personnel are selected to perform the assessment. If a major network enhancement is anticipated as a result of step 5, the information technology assessment, consider hiring a network engineer on a permanent basis.

The following is a list of responsibilities and skill sets for each of these three roles. Knowledge of law enforcement operations also is essential to all of these positions. Technologists should never work in a vacuum. They have to understand law enforcement needs, specifically, your needs. Otherwise, the technical help will be entering another world, with new vernacular. Sound familiar?

Data Analyst

Responsibilities:

- Analyze flow of information in the organization.
- Determine the sources of applicable data and the processes that use and/or modify the data.
- Evaluate as-is (current) systems for records management in terms of data integrity, accessibility, and security, and identify opportunities for improvement in these areas through modernized software, integration, and/or process improvement.

Skills, training, experience:

- Excellent communication skills, both verbal and written.
- Prior experience in database engineering with working knowledge of relational database design concepts and structured query language (SQL).
- Working knowledge of 911 CAD and RMS.

Business Analyst

Responsibilities:

- Objectively analyze current business practices, policies, and procedures.
- Streamline the business processes after thorough examination.
- Generate as-is and to-be (future) models along with written text to support and enhance the models.
- Provide updates to agency policies and procedures for implementation of new business processes.

Skills, training, experience:

- Excellent communication skills, both verbal and written.
- Prior experience in business process reengineering.
- Working knowledge of 911 CAD and RMS.
- Working knowledge of mobile communication systems.
- Working knowledge of word-processing systems and modeling software.

Network Engineer

Responsibilities:

- Objectively analyze current network infrastructure, computer equipment, and software.
- Determine the needs and system resource changes with recommendations for system upgrades and procedures to administration.
- Determine hardware and software requirements, evaluate equipment options, and make purchasing decisions.
- Provide system policies and procedures and associated documentation.

Skills, training, experience:

- Knowledge of network infrastructure and equipment to include routers, bridges, hubs, switches, and system interfaces.
- Working knowledge of network software (Novell Netware®, Microsoft® Windows NT®, and/or UNIX® and fileserver hardware.
- Working knowledge of PC applications software (Windows® 95 and above and/or Windows NT, major-brand word processor, major-brand spreadsheet or database, e-mail systems, and modem communications programs).
- Working knowledge of 911 CAD and RMS.
- Working knowledge of voice communications systems including privacy voice exchange (PBX), voice mail, call accounting systems, and public and private telecommunications systems.
- Working knowledge of mobile communication systems.
- Excellent communication skills, both verbal and written.

Any assistance you receive should be of a completely unbiased nature, regardless of the degree of project complexity. If the project requires the assistance of outside consultants, their qualifications should be known or determined. Most importantly, ensure that their previous efforts did not always result in the selection of the same components or vendors.

Typically, the acquisition of a complex system requires the approval or concurrence of other agencies or departments. If a police department is acquiring a complex IT system, it probably will need approval and concurrence from the city's purchasing department and attorney, as well as approval from the city council and/or mayor or city manager. Using experienced, unbiased, outside assistance can make this approval cycle much smoother.

Step 3. Form a Working Group

A complex IT project will involve a variety of technical and nontechnical personnel. Once the scope is determined, individuals with appropriate experience who will be responsible for the assessment and evaluation can be chosen for a working group.

Regardless of the scope of the project, you will need to determine what system capabilities you have, what the new system must do, what the system will cost, and how long it will take to acquire and make operational. Typically, if you have hired outside help, they will provide or acquire most of this information.

Build a team of agency people to help with the task of understanding user needs and interfaces. This group should include persons familiar with all the disciplines within your system. It should be chartered by senior management to help you deliver a system with a minimum risk of failure. It will be the job of this group (or subsets of this group) to work with the data analyst, business analyst, and network engineer to help conduct the information technology assessment and develop the system needs, RFP, interfaces, estimates of cost, and schedule. Most likely, you will need to establish one person as the project manager to oversee the entire process from the initial assessments through implementation.

Step 4. Educate Your Team

To understand the importance of this step, we must jump ahead for a few moments. During the IT project plan the team will be determining the current status of the agency's information processing "system" and developing the as-is snapshot. Next, the

team will need to determine what the new system should be and how end users will employ the new technology. How can they make decisions on a new system if they do not know what is possible?

In certain instances, the proposed system may be so technically complex that they cannot determine the needs because they do not understand the possible solutions. If this is the case, it now becomes necessary to educate the team. The business analyst, data analyst, and network engineer will be able to provide valuable input in their areas of expertise and can assist in educating the team as a whole.

It is important to remember that this step is not meant to be a decision point. The education process can be handled in a number of ways, including:

- Presentations on the existing system and information interfaces within the agency.
- Presentations on planned and funded upgrades.
- Product demonstrations from invited vendors.
- Information gathering at conferences and shows.
- Information gathering from product databases.
- Information gathering over the Internet.
- Surveys and site visits with agencies using similar technologies.

At this point, a potential pool of vendors may already be identified for your basic needs. A very effective tool at this time is to develop a Request for Information (RFI) document and send it to these potential vendors. An RFI can be a very simple, no-obligation document requesting information about a vendor's products to meet your needs. The responses will range from product brochures, to prepared responses, to sales representatives on your doorstep.

Step 5. Conduct an Information Technology Assessment

Many project plans go straight from educating the working group to developing the requirements of a new system. The assumption that you will *know* what you need has been a big pitfall in many IT projects. The information technology assessment is the bridge between these two steps and should be executed prior to defining requirements for a new system.

The information technology assessment is a methodical process to help determine what your business processes are, which ones are key to the agency's operation, and *how* you process information in your agency. It combines reviews of an agency's current policies and procedures, business processes, information technology infrastructure, software (RMS, CAD, etc.), and hardware. In short, it provides a baseline of where you are now and helps to pinpoint areas for improvement.

Since this step is a long and involved process, we have dedicated the next chapter, Conducting an Information Technology Assessment, to the particulars. As we continue through the project planning steps, remember that having completed step 5, you will have a much clearer understanding of where technology can best benefit your agency.

Step 6. Develop Overall System Needs

The overall system needs should be determined from the results of the information technology assessment. As your team members develop system needs, it is of utmost importance that they do not come back with specific solutions.

This **is not** a need: *A PC running Microsoft Windows with Acme Report Writer V3.0 software.*

This **is** a need: *A system to quickly and accurately input information in the field that can be transferred to an existing crime reporting system at the station.*

Keep in mind that these needs are *overall* system needs. The result will probably be a complex system that could not realistically be implemented or funded in one step. You may have the inclination to make concessions for your needs. Do not fall into this trap. Rather, state your desired goals, but realize that you will accomplish them through a series of phases. In the next step, you will determine what those phases

are. This overall system design will also serve as parameters for developing system requirements in an RFP process.

The ability to articulate user needs is almost an art form that takes time to develop. The raw data your team collected during the information technology assessment and the results of the assessment are used to develop the overall system needs.

Step 7. Develop a System Design and Schedule

Developing a system design and schedule most likely will be done simultaneously with developing a cost estimate (step 8). You will need an idea of cost as you design your system and timeline.

The design of the system is the job of the working group, including the business analyst, data analyst, and network engineer. If you have not hired these positions or do not have them on staff, then it is your job. Develop the system design and schedule based on the overall system needs. Now comes the difficult part of assigning priorities to needs, and cost is an obvious factor. Unfortunately, the "big picture" may be beyond your budget, so you will need to make some tough decisions. Work in all of your system needs using phases. Do not worry that phases may extend into the distant future. It will be easier to lay the groundwork in the early phases if you know where you would like to be down the road. For example, if you know you would like to implement mobile data computing in phase II, ensure that the server hardware you purchase in phase I will be able to accommodate this upcoming equipment.

You will want to ensure that the design is realistic. The more complex it is, the more complex this review will be. If you have a list of potential vendors, you can either convene a design conference or send your design to your vendor pool for comments. It is reasonable to expect that vendors will have the necessary technological experience for this task. You also will have to develop a top-level schedule of the estimated time needed to complete the phases.

Step 8. Develop a Cost Estimate

Once the design is complete, the costing should be straightforward. Cost estimates can be found informally by talking with other agencies that have installed similar systems. More formal cost estimates come from the actual vendors. In those instances in which the system can be well defined, you can ask your vendor pool for price quotations. This is best accomplished through the creation of a Request for Quotation (RFQ). Although this document is nonbinding on the vendor, it does tend to establish the estimated system cost for a limited period of time. Usually, the vendor will indicate the timeframe in which the quote is valid. You should also develop a document detailing where you are obtaining the funds to implement the initial phases of the project. This document should include limitations of the funding sources and, if required, the deadline for expending the funding.

As mentioned above, steps 7 and 8 will most likely be executed simultaneously. Since your design and schedule have been based on available or anticipated funding, developing a total cost estimate is a matter of bringing all the pieces together. Each phase should receive its own cost estimate.

Step 9. Obtain Management Approval

This is the point to bring senior management and outside agencies into the picture. Senior management must understand:

- System costs.
- System capabilities.
- The estimated schedule to completion.
- The consensus of your working group and stakeholders.
- The next steps.
- The help you will need from senior management.

When management gives approval to proceed, you should next educate other departments, such as purchasing and legal, as to the system design and intentions. If the system requires a formal procurement process, your documents will need input and approval from these groups. It is important to establish positive relationships with these people. Solicit their concerns, experiences, and requirements. Try to establish a single point of contact within each agency and have them estimate their time for tasks that will be assigned to them.

You may be able to purchase and install a less complex system without a formal evaluation. However, a complex system will require a methodical evaluation of possible solutions—the RFP process. The development and issuance of an RFP is no small task. Later chapters of this document have been dedicated to steps 10, 11, and 12—the development and evaluation of an RFP, the selection of a system, and system implementation.

In the next chapter we discuss the details of the information technology assessment (step 5).

Chapter 3. Conducting an Information Technology Assessment

In the last chapter we briefly discussed the information technology assessment. This assessment requires an indepth review of business processes to determine how you currently use technology and to pinpoint where technology can provide the best benefits. By conducting this assessment before determining needs, you will be better able to implement technology solutions in the most effective way.

The information technology assessment is a complex process, so we have broken it down into four components:

1. Review your agency's business processes and procedures and determine which ones are the "core" processes.
2. Develop pictures of the core business processes—the as-is maps.
3. Analyze the as-is maps to determine ways to streamline these processes.
4. Use this information to develop pictures of the more efficient processes—the to-be maps.

For example, let us assume the incident report process is a core process in your agency. The as-is map for this process may show that your officers conduct separate inquiries at the local, State, and Federal level for criminal history. Therefore, the as-is map is showing a piece of the process that could be improved. Perhaps a new software application could allow the officers to conduct one inquiry and retrieve the information from all of these entities at once.

Let's take a closer look at these four components and how to work through them.

Determine the Core Business Processes

A business process is a collection of related, structured activities—a chain of events—that produce a specific service or product for a particular customer or customers. A business process is characterized by these factors:

- A start, an end, and a purpose.
- Clearly defined inputs and outputs.
- Value added from the resulting output.

Why is it important to review your agency's business processes for an IT project? The introduction of new or improved information technology often requires changes to the policy and procedures within the agency in order to take full advantage of the efficiencies created by the technology. These changes may be minor or major. The business process review provides the opportunity to "see" how your agency operates and improve the processes *before* the technology is implemented. Do you really want to spend the time and money to automate an inefficient or unnecessary process?

Together, all of the business processes in an organization form a total delivery system for products and services. Processes that are the most vital for mission performance and organizational survival are considered **core processes.** However, some processes may not be relevant to the scope of the project that you have previously defined. Therefore, the identification of the core processes should be done with respect to the project. The primary focus of the core processes should be relative to information services and products within the agency that pertain to mission critical activities.

For example: Responding to a call for service is vital to an agency's mission; hence, it would be considered a core information process and should be selected for review. Tracking agency-owned property, while important to budgetary impact, may not be perceived as a mission-critical process. Therefore, tracking agency-owned property might not be viewed as a core process.

The Initial Core Process Review

A core process review requires analyzing the fundamental processes of an organization from a cross-functional perspective. The working group should analyze existing processes until the group clearly understands what the processes are trying to accomplish. The point of the review is to understand the purpose of the process. The initial process review is considered the baseline. The remainder of this chapter assumes that the working group will participate in the entire technical assessment.

How do you start?

First, gather information for each core process by surveying and interviewing officers and staff to determine standard practices. To prepare for the interviews, create operational scenarios that are relevant to the function or task and distribute these to the end users prior to the surveys or interviews. End users may be grouped by function, department, or geographic location. Next, develop focused surveys and distribute these to the interviewees. The surveys are intended to uncover current system operations and shortcomings, as well as provide ideas for future system needs. Interviews should be used to clarify or substantiate survey results. Often, the survey responses will identify unexpected results requiring that additional details be discussed and documented.

The working group should also be sensitive to the operational needs of the agency and make interviews as concise as possible. A solid commitment is required from managers to ensure that adequate time is provided to complete the interviews.

Next, review policy and procedures that direct the processes. Many times end users will have valuable suggestions for policy and procedural changes that the introduction of new technology may bring. These need to be specifically documented and included in the final recommendations.

Finally, review current information technology infrastructure and current computer applications. This will include a review of your network infrastructure, computer equipment, and applications in terms of data integrity, accessibility, and security.

Develop As-Is Process Maps

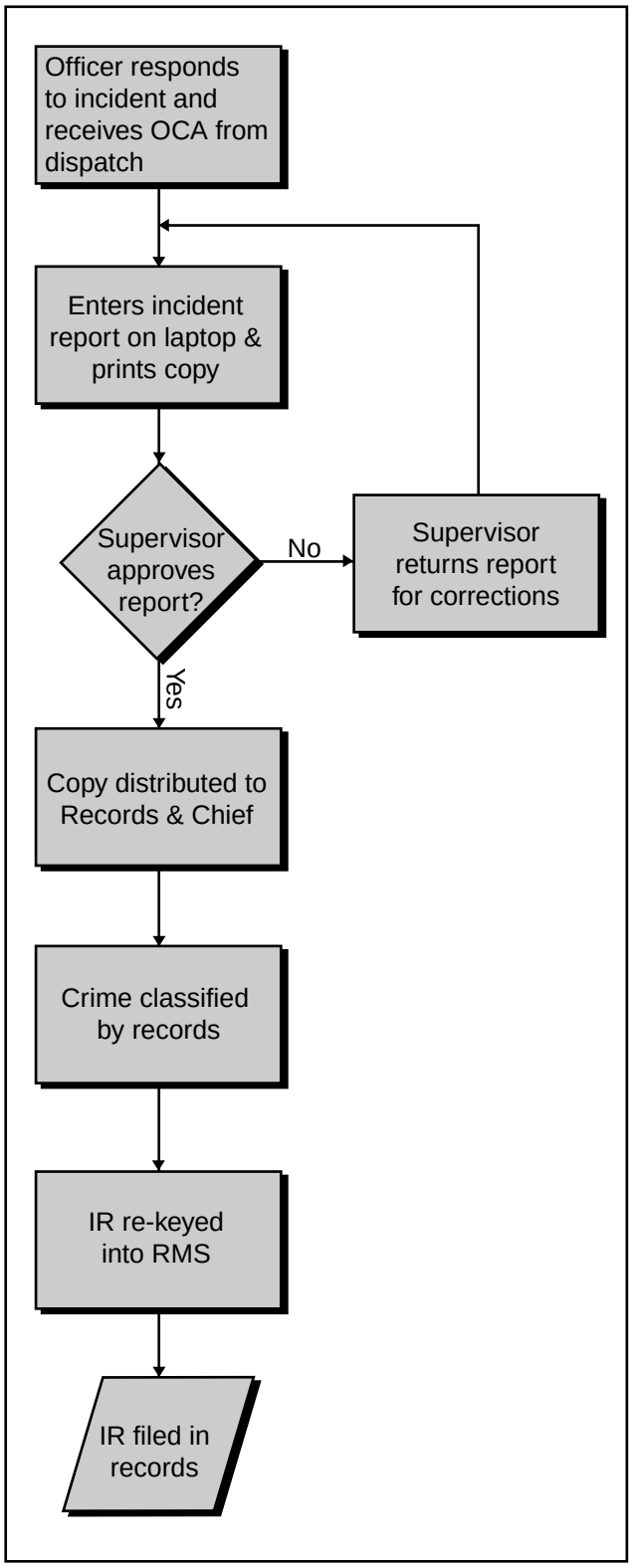
An as-is process map is a graphical representation of how business information flows. The map depicts the chronological steps of the inception of the information, who handles the information, and how the information is transformed at each step. It is used to establish a baseline for subsequent business process improvement models. Exhibit 3–1 is an example of an incident report as-is process map. It clearly focuses on the key steps in the chain of events. Insignificant steps should be eliminated from the process map.

Along with the process map, text is written to enhance the understanding of how and in what format the information is introduced to the process, stored or filed, and retrieved for reporting purposes. A process map of an incident report may include steps for generating an incident report on a form, storing the information in an RMS, and then filing the report in a cabinet. However, it may be illogical to include all of the possible uses of the incident data in the map. For example, an investigator may need to query the data by criteria different than a person querying the data to generate Uniform Crime Reports (UCR). The following is a sample of the text that might accompany the above process map. The text that supplements the incident process map clearly identifies how the data is processed and the problems that exist within the process.

Form Filler is a tool that allows an electronic form to be created and data to be entered into the form on a mobile computer. Data is not electronically transferred to the AS/400. An incident form was developed by the PD and allows an officer to enter incident reports, then print the reports for supervisor approval. The supervisor approves the report, then delivers the printed copy to Records. Records adds the UCR code, then re-keys the data into the RMS. This process includes duplicate typing of the incident report.

Investigators maintain case status on a log sheet. Investigators do not rely on query results related to cases in the RMS. Query results often produce an incorrect number of records when many records exist or produce incorrect records on searches performed by name, date of birth, address, and physical description.

Exhibit 3–1. As-Is Incident Report Process Map



The Second Core Process Review: The Analysis

What do you do with the as-is process maps?

The as-is process map and accompanying text are analyzed to determine where steps that do not add value exist in the process and to identify primary versus secondary activities that directly support the technology objectives. The next step is to compare the as-is process maps and text to "best practices" of other agencies, combined with a review of the network infrastructure, information systems, and agency policy. During this review the team begins to formulate solutions to support the modernization objectives. A second review should reflect process improvements, changes as they relate to a total information technology infrastructure, and areas where new technology can replace outdated methods.

The team should seek to determine which steps in a process really add value and search for new ways to meet the agency's objectives. Throughout the review the team members should ask "why" and "what if" to analyze the purpose of each step.

The surveys and interviews done previously should identify problems and shortcomings of the current systems. It is important to include evidence of problems when it is available since it provides specific instances of system performance. End users should be given the opportunity to grade or evaluate current system features. This will help highlight unwanted or unused capabilities that can be updated or eliminated in the to-be process.

Although end users may not know the specific or technical requirements for a future system, they can help the working group identify the operational needs of the agency. End users should be given the opportunity to suggest features or technologies not otherwise available to them.

The second review should culminate in the development of the to-be maps that depict how the business process could be streamlined by eliminating non-value-added steps in the process or by replacing steps with up-to-date technology.

Develop To-Be Process Maps

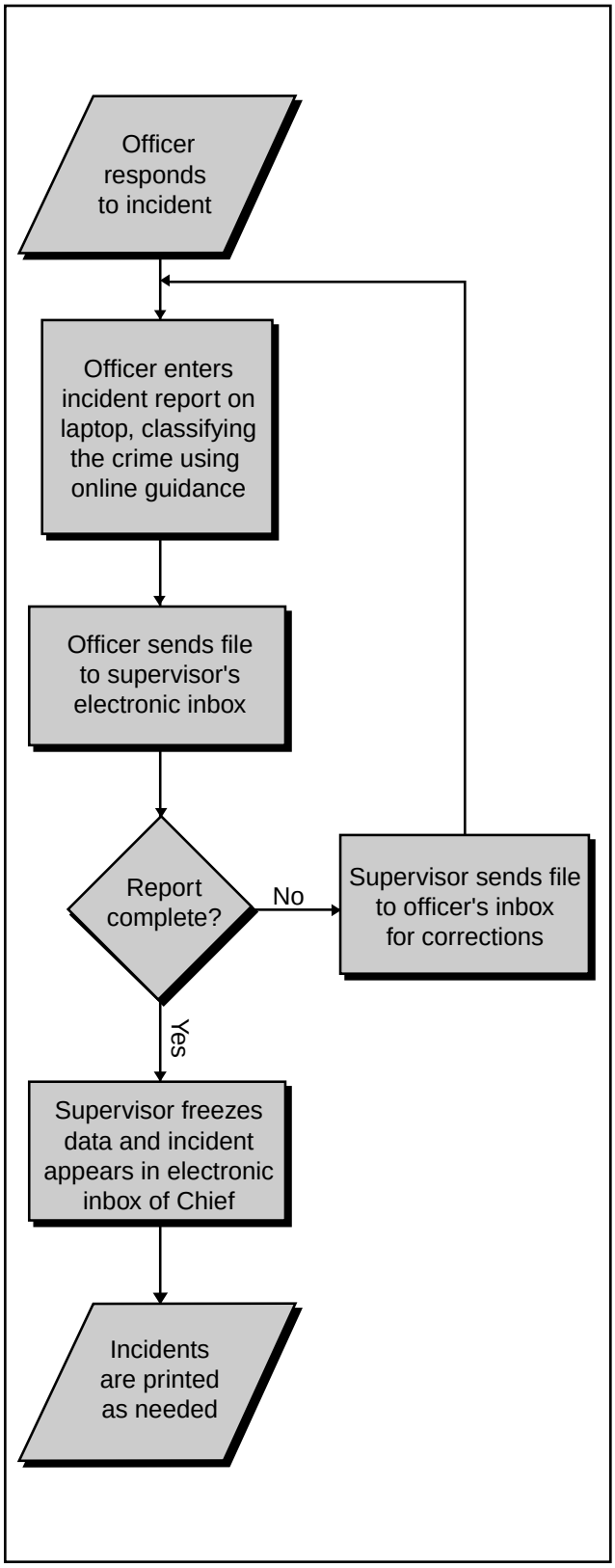
The to-be process map is a graphical representation of how business information should flow after changes to the process have been implemented. The to-be process map shows where activities can be streamlined and where new technology can replace outdated methods. Text should be written to accompany the to-be process map to clearly explain how the implementation of new technology will meet the agency's modernization objectives. Details from the technical assessment should be recorded in a report that is easily understood and clearly defines the agency's needs. Results of the technical assessment should be used as a guide when developing the overall system needs (step 6) for the technology that will be implemented. The to-be maps and text can also be used to provide support for writing specifications and requirements for inclusion in an RFP (See chapter 8).

Exhibit 3–2 is an example of a to-be map that includes steps that will improve the process and take advantage of modern technology.

The information technology assessment is a long and involved task within the entire project plan. With so many ways to automate individual tasks and technology tools available to single departments, it is easy to lose sight of the importance of an integrated system that works for the whole agency. Developing system needs becomes less cumbersome if you examine how your department works and where you could inject improvements.

We will now look at the three main components of a law enforcement IT system: application software, hardware, and mobile data communications. Understanding these components is crucial to writing an appropriate RFP and a successful implementation of a system.

Exhibit 3–2. To-Be Incident Report Process Map



Chapter 4. Law Enforcement Information Systems: A Look at Application Software, Part I

The first component of a law enforcement information system that we will discuss is application software. This software may be off the shelf or software that is customized for your agency. Regardless of origin or complexity, you must consider the entire scope of the application's impact on your agency. In this chapter we review applications that are common to most law enforcement agencies, RMS and CAD, and discuss how to begin evaluating them. This chapter can be used as a reference when defining requirements for an RFP. In the next chapter, we will overview two applications that are quickly becoming mission-critical for law enforcement agencies, geographic information systems and crime mapping systems.

Before we discuss RMS and CAD applications in detail, we will look at the interoperability between these law enforcement applications and between your agency and other entities, such as the fire department, emergency medical services (EMS), or courts. We also will tackle some general operational specifications to keep in mind when choosing any software application.

Interoperability

In the IT project plan, you determined your overall system needs (step 6) and your system design (step 7). Most likely, this identified the types of systems or modules expected to be delivered, such as CAD or RMS. In the requirements stage, you should clearly state the expectations of the interoperability between the modules.

Agencies that are expected to be a part of the overall system should be identified. If your plans include interoperability with the police, fire department, EMS, courts, or other agency systems, this should be clearly stated in the interoperability description.

To be fair to proposing vendors and to ensure a successful implementation, information about existing systems and interfaces to those systems is needed. Information should consist of at least the descriptions of existing hardware, software, and database characteristics; models or structures of databases; and constraints or assumptions of those systems. The following is a list of questions that you should answer in the interoperability section of the specifications.

- Are all of the modules being replaced? If not, should the existing modules be integrated to the new modules?
- Will data be shared between the modules? If so, what data?
- Will RMS, CAD, enhanced 911 (E911), court systems, mobile data systems, or GIS be integrated?
- If all of the modules are being replaced, will existing data need to be migrated to a new system?
- Who is expected to perform data migration?
- Will all of the existing data be migrated to the new system?
- Will there be any system down time during the installation of new systems?
- Will any of these systems be shared with other jurisdictions? If so, what data should be private within an agency, and what data can be shared among agencies?
- Will any of the new systems be integrated with State or Federal systems, such as NCIC or NCIC 2000?
- If an interface for NCIC queries is included, should the user be able to query the local RMS with the same query as NCIC?

You should be prepared to answer more specific questions about interoperability between specific systems, such as:

- What should happen to the interaction of the systems when one system fails?
- What are the expectations if the CAD system fails?
- Will addresses be verified and standardized using GIS?
- Will one unique case number be generated and shared between the integrated systems?
- Will data that is entered into a CAD system be entered again for the RMS?
- Is the master name or location data shared between systems?

Advanced Resources

Previously submitted RFPs are the best resources when deciding the details to be included in your system requirements. The Town of Mt. Pleasant, South Carolina, wrote an effective RFP for a new CAD, RMS, and mobile data terminals (MDT) that details the desired interoperations between the systems. This proposal supplies excellent descriptions of their expectations for name, location, and property table requirements in addition to the reports they expect to be available online. It can be viewed at www.nlectc.org. Other RFPs can be viewed at www.search.org under the "IT Acquisition Database" link.

General System Specifications

General system specifications should be incorporated that apply to any systems being implemented. The general specifications should portray the overall look, feel, and response of the system. These are very important for the future use of the system and must be clearly communicated to vendors. Standards prospective vendors must meet should be defined in this chapter. Vendor characteristics such as customer contact references, user groups, customer support, and licensing issues should be included as requirements. Examples of general system specifications include (but are not limited to):

Vendor/System Qualifications

- The system should be built using open standards.
- The vendor should employ well-defined, widely used interfaces, communication protocols, and programming languages.
- The vendor should employ standards that have been adopted by recognized standards bodies such as the International Standards Organization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the American National Standards Institute (ANSI), and OpenGIS.
- The vendor should have a well-defined software development process. Certification in SEI (at least level 3) or ISO 9000 is a plus.
- The system should employ a relational database that supports SQL.
- The vendor should provide a data dictionary to users and provide for access to the application's data without depending solely on the vendor's interface (e.g., compatible with widely used third-party tools for ad-hoc query and report generation).

User Interface

- The application should provide a graphical user interface where applicable.
- The interface should provide seamless screen navigation based on operation in process (e.g., automatically opening a name window as an incident report is entered).
- The interface should support generic operations for text (e.g., cut, paste, copy).
- The interface should support multiple input techniques—mouse menu selection and/or keyboard.
- The interface should have multiple options for accomplishing a task (menu selection, button, and/or accelerator keys).
- The interface should provide "undo" mechanisms to allow the user to reverse an operation.

Easy and Accurate Input

- The system should not require duplicate entries of data. For example, once a person's name, date of birth, sex, race, or other common data have been entered in an incident report, that person would only have to be referenced in subsequent reports.
- The system should provide for effective search capabilities:
  - Soundex searches (e.g., Smith vs. Smythe).
  - Similar name searches (e.g., Jim vs. James, Chuck vs. Charles).
  - Wildcard searches (e.g., Kat* would match Kathy, Katherine, or Kate).
  - Exact match searches.
  - Text searches of narrative data.

Error Checking

- The application should provide data validation where applicable. Where possible, data entry errors should be prevented as opposed to generating error messages after the fact. Error messages should be specific and meaningful to the party responsible for correcting the problem.
- The system should provide spell check with a user-configurable dictionary.

Help

- The system should provide online help and context-sensitive printed user manuals.

Flexibility

- The system should use master tables for fundamental entities such as persons, addresses, vehicles, boats, and property so that these entities can be efficiently linked. The system should provide the capability for authorized users to efficiently merge these entities if duplicates are entered in error.
- The system should provide ad-hoc query capabilities in which users can develop and save their own queries with minimal training, and the underlying database should be supported by common ad-hoc query and report generation tools.
- The system should be able to process both 20th and 21st century dates without distorting the results, losing information, or otherwise causing data corruption.

General Operational Specifications

Operational specifications include, but are not limited to, system reliability, response times, and security. Requirements for individual systems may further delineate each of these topics as necessary.

System Reliability

- The system should be capable of providing 24-hour, 7-day (24/7) operation. For example, the system should allow the performing of backups while the system is in use.
- What constitutes a system failure and how the failure should be managed should be defined.
- The amount of acceptable down time per month should be specified.

System Response Times

Acceptable response time should be spelled out in the specifications, such as:

- Time to display person information.
- Time to display arrest information.
- Time to display location information.
- Time to display names associated with an address.

System/Network Security

- The system should be protected from unauthorized entry/access.
- Only users with valid user identification and passwords should be allowed entry into the system. Passwords must be encrypted.
- The system supervisor shall have a separate user ID and password that permit him/her to perform system administrative functions.

- The system supervisor should be able to add and delete users.
- Each user should have a separate account for which his/her privileges are defined.
- The system should provide security and referential integrity at the database level, rather than at the application interface.
- The system should provide for transaction logging.

Records Management System[1]

An RMS is an agencywide system that considers the reasons, the processes, and the means necessary for a document to exist and be used. RMS must cover the entire life span of the document, from its generation to its destruction. The system provides for the effective storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files that are related to a single subject.

For the purposes of our discussion, we are concentrating on records related to law enforcement issues. These records could include incident reports, law enforcement personnel records, criminal records, and crime analysis.

An RMS allows one source of data input and multiple reporting mechanisms while enabling an agency to deal with its records in a simple environment. It should provide the ability to generate crime statistics for UCR or NIBRS.

Who Uses the RMS?

It is essential that end users of the system be involved as early as possible in the planning process so that they have a stake in the system and that viable and acceptable systems are implemented. The following personnel could be end users of an RMS:

- *Patrol officers* provide the primary input to the system and their participation is vital to ensure report accuracy and completeness.
- *Records personnel* use an RMS for data entry, inquiry, and retrieval.
- *Investigators,* who represent a primary set of end users, require records for building cases and filing cases.
- *Crime analysts* have a different set of requirements and are concerned with the availability of accurate crime information to perform complex analyses of crime patterns.
- *Command personnel* use the system to meet their management information needs.

Objectives

The objectives should come into focus during the technical assessment and should be of assistance in developing specifications. The objectives for installing an RMS must be clearly stated when defining what you want an RMS to do for your agency. Examples of objectives for an RMS include:

- Improve the accuracy and reliability of information within the agency by consolidating departmental records.
- Reduce the cost of data entry by eliminating duplication of efforts.
- Provide a consistent chain of reporting and analysis.
- Expand the use of the system departmentally by providing a system that is easy to learn and use.
- Minimize data handling.

Functional Specifications

The functional specifications for the RMS define what the system should do, not how it should be done. You will want to be able to collect, store, retrieve, analyze, and report the information that pertains to the activities of your agency. Bear in mind that pattern prediction capability may well become a requirement of the system upon implementation. General functions that should apply to all agency activities stored in an RMS should be presented at the beginning of the functional specifications. The following are examples of general RMS specifications.

[1] Some of the information related to the RMS definition and who uses an RMS was based on the "Law Enforcement Information Management Section" of *Guidelines for Records Management Systems* (International Association of Chiefs of Police).

General RMS Functions

- The system should link persons, addresses, property, and vehicles (including airplanes and boats), if required, to each event.
- The system should allow for retrieval of information by one or any combination of the elements or events.
- The system should be capable of generating a printed report for each event.
- The system should be capable of linking a case number to each event.
- The case number should be displayed on the event screen and on the printed report.
- The system should provide an audit trail of name and address searches for NCIC.
- Information that is common across many RMS functions includes name, location, vehicle, and property. An RMS should contain "master" tables for this information so that data is not entered multiple times for each function. Specific exceptions to the handling of this data in any function should be clearly defined.
- For each of the functions below, requirements should be written based on the agency's specific needs. These requirements could include a general description, major functions and types of data, reports and screen views, dissemination of data, and report writing.
  - Incident reporting.
  - Field reporting.
  - Investigative case management.
  - Traffic management.
  - Crime statistics.
  - Officer activity.
  - Criminal records.
  - Crime analysis.
  - Gang activity analysis.
  - Evidence.
  - Juvenile records.
  - Inquiries, including mobile data inquiries.
  - Missing persons.
  - Warrants.
  - Narcotics.
  - Vehicles.
  - UCR/NIBRS.
  - Sex offender.
  - Known associates.
  - Licenses and permits.
  - Neighborhood organizations.
  - Personnel scheduling.
  - Training/qualifications tracking.
  - Agency-owned property tracking.

Computer-Aided Dispatch System[2]

A CAD system allows emergency operations and communications to be augmented, assisted, or partially controlled by an automated system. It can include, among other capabilities, computer controlled emergency vehicle dispatching, vehicle status, incident reporting, and management information.

A CAD system could be interfaced to an E911 system that provides automated routing of emergency calls to public safety answering points through a specified telephone service area.

Who Uses CAD?

The following is a list of primary and secondary end users of the CAD system:

- *Call takers/dispatchers/supervisors* have a significant impact on field personnel and the public. They have the greatest interaction with the CAD system and E911 systems. They are key players to successful system implementation.

[2] Some of the information related to the CAD definition and who uses the CAD was based on the "Law Enforcement Information Management Section" of *Guidelines for Computer-Aided Dispatching Systems* (International Association of Chiefs of Police).

- *Officers in the field* are primary users because they are the personnel most impacted in the dispatch process. They are required to utilize mobile data terminals or computers for many CAD functions and are key for a successful system implementation.
- *Records personnel* represent users with major input in the CAD reporting process. They could supply the definition of the interfaces to an RMS and the requirements for CAD data transfers.
- *Command staff and planning staff* have a need for statistics, management information, resource deployment data, and ad hoc reports.
- *Network and telecommunications staff* are the technical personnel who will operate the system, provide ongoing maintenance, and have input into the requirements for those elements of the system.

Objectives

The objectives should be defined during the technical assessment and will assist in developing CAD specifications. They place boundaries on the system and provide the base direction for systems design. The objectives for implementing a CAD should be clearly stated when defining what you want the CAD system to do for your agency. Examples of objectives for a CAD system include:

- Streamline the processing of emergency calls for service from the public and improve the ability to handle peak call loads.
- Increase officer productivity and provide better resource management.
- Enhance officer safety with detailed information on call locations and involved persons.
- Simplify the unit status monitoring function and relieve telecommunicators of some of the workload by supporting direct entry of status information from the field.
- Provide the capability for agency employees to make various database inquiries.
- Provide accurate, up-to-date information for management control.

Operating Environment

Agencies and jurisdictions intending to use the CAD system should be identified. The following provides insight to the agencies current operating environment. Proposing vendors will use this operational configuration to determine the hardware and software requirements of the system. This information shall also be used to determine the system loading level to be used during the system response time test. Peak hourly loads shall be calculated at 10 percent above the average daily load figures. These figures should be in the specifications for:

Police/Sheriff

- Patrol operations:
  - Number of members in the department.
  - Number of members in patrol.
  - Patrol officers on duty per shift.
  - Number of marked, controlled vehicles.
  - Number of special units controlled.
- Communications operations:
  - Number of dispatch positions. (If these are not single positions, explain. If dual, do both operators dispatch?)
  - Number of call-taker positions.
  - Number of remote locations (explain functions required at remote locations).
  - Number of telephone report positions.
  - Number of communications supervisor positions.
  - Number of personnel in communications (total per shift).
- Average daily volumes:
  - Calls for service.
  - Incidents based on calls for service.
  - Traffic stops.
  - Officer-initiated incidents.
  - Incoming E911 telephone calls.
  - Incoming seven-digit telephone calls.

Fire Department

- Field suppression operations:
  - Number of sworn members in the department.
  - Number of sworn members in suppression.
  - Number of stations.
  - Number of engines (pumpers).
  - Number of trucks (ladders).
  - Number of other units controlled.
- Communications operations:
  - Number of dispatch positions. (If these are not single positions, explain. If dual, do both operators dispatch?)
  - Number of call-taker positions, if dispatchers do not act as call takers.
  - Number of remote locations (explain functions required at remote locations).
  - Number of personnel in communications (total per shift).
- Average daily volumes:
  - Calls for service.
  - Incoming E911 telephone calls.
  - Incoming seven-digit telephone calls.
  - Incidents based on calls for service.

Emergency Medical Services

- Field operations:
  - Number of stations.
  - Number of public ambulances.
  - Number of private companies dispatched.
  - Number of personnel per ambulance.
- Communications operations:
  - Number of dispatch positions. (If these are not single positions, explain. If dual, do both operators dispatch?)
  - Number of call-taker positions if dispatchers do not act as call takers.
  - Number of remote locations (explain functions required at remote locations).
  - Number of personnel in communications (total per shift).
  - Number of ambulance zones.
- Average daily volumes:
  - Calls for service.
  - Incoming E911 telephone calls.
  - Incoming seven-digit telephone calls.
  - Incidents based on calls for service.

Functional Specifications

The functional specifications for the CAD should define what the system should do, not how it should be done. You will want to be able to provide the agency with the capability to effectively serve the emergency needs of the community. CAD systems are designed to dispatch resources automatically or to assist a call taker in dispatching resources. The system should be equipped to record all calls for service, maintain accountability of on-duty personnel, and provide resource information to management. It should render a detailed audit trail of all accessed data and store information that will allow for report retrieval by a variety of methods. General functions that should apply to all call-taking and dispatching activities should be presented at the beginning of the functional specifications. The following are examples of general CAD specifications.

General CAD Functions

Listed below are a few general CAD requirements, which may or may not apply to your situation. They are to be used as examples and are not all inclusive.

- Call-for-service data are collected during the call-taking and dispatching operations. Upon disposition of each event, the CAD system should pass the call-for-service data to the RMS.
- The CAD system should assign report numbers since most formal report numbers are assigned during handling of the dispatched event. All the other modules will have access to the CAD report number. Since some events ultimately result in court proceedings, the RMS must be able to integrate this information into the court files.
- The Geo/Street Index should be maintained as part of the CAD system.

- Key addresses, such as incident location, must be address verified and the system must calculate or assign the associated reporting district codes (track number/patrol neighborhood).
- The interaction between the user and the computer should be via preformatted, fill-in-the-blank video screen layouts. This computer-user interaction occurs immediately (real time) so that transactions, which add to or change the database, are applied as they are received. Any subsequent retrieval will display the current information.
- The system must have a built-in archiving capability.
- Information that is common across many CAD functions includes: date/time display, address validation, street aliases, and intersections. The CAD system should contain "master" tables for this information, so that data are not entered multiple times for each function. Specific exceptions and handling of date/time display, address validation, street aliases, and intersections data and their associated data should be clearly defined.
- For each of the functions below, requirements should be written based on the agency's specific needs. These requirements could include a general description, major functions and types of data, reports and screen views, dissemination of data, and report writing.
  - Duplicate call detection.
  - Date and time display.
  - Address validation (street aliases, common place names, intersections).
  - Call-taker functions.
  - Event routing.
  - Interaction with E911.
  - Dispatch capabilities.
  - Resource recommendations.
  - Notification procedures.
  - Fire dispatch functions.
  - MDT functions.
  - Remote site functions.
  - Priority incident interrupt.
  - Map display.
  - Out of district display.
  - Administrative scheduling capabilities.
  - Maintenance functions.
  - Wrecker rotation.
  - Event recap reports.
  - Time analysis reports.
  - Management reporting.
  - Premise history/hazard inquiry.
  - Personnel file.
  - Business "Rolodex®" file.
  - Catastrophic event processing.
  - Automatic vehicle location system.

Chapter 5. Law Enforcement Information Systems: A Look at Application Software, Part II

Geographic information systems and crime mapping are fast becoming mission-critical applications in law enforcement agencies. Since these systems may be new additions to many agencies, we have provided an overview of what the systems can do and a starting point as you consider adding these systems to your information technology network. Due to the complexity of these systems and the individuality in solutions, we have not provided specifications as we did in the previous chapter.

Geographic Information System

The introduction of electronic maps has been a welcome addition for many emergency service agencies. A GIS is a computerized system for linking and analyzing map data and related tabular database information. It is used to capture, manage, manipulate, and display spatially referenced data in the electronic format. Think of a GIS as an electronic stickpin map. A GIS can assist your agency's operations in the area of planning, management, and crime mapping.

A GIS provides a digital representation of the Earth's surface. There are many different formats and types of digital maps available. Therefore, before you can choose a GIS, you will need to determine how you will use the system and interfaces to any other software you require. A GIS as a tool can be used to perform various functions with the data resulting in new types of displays. The data is built upon layers of information as depicted in exhibit 5–1. ESN boundaries are emergency service number boundaries used to determine which agency answers a 911 call.

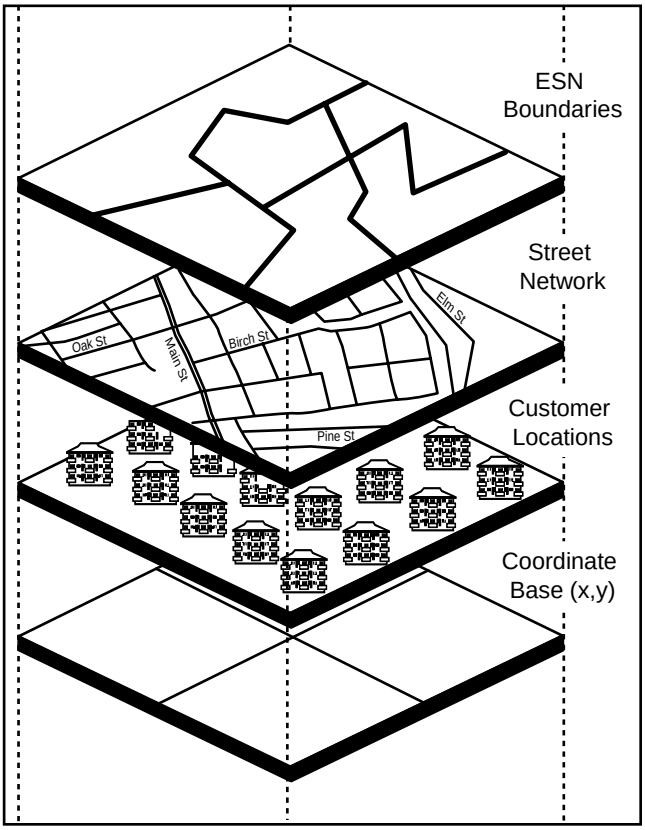
Who Uses a GIS?

- Electronic maps or a GIS can be used in a dispatch/911 center to show call takers and dispatchers the exact location of calls for service, apartment complex layouts, and floor plans.
- A Global positioning system (GPS) or an automated vehicle locator (AVL) system uses a GIS to monitor patrol unit whereabouts and assist in recommending the closest unit.
- Probation and parole departments are looking to GIS and GPS to triangulate the whereabouts of convicted offenders in lieu of incarceration—referred to as electronic home monitoring.

The Steps To Developing a GIS

1. Determine if you need to purchase external geographic data. Geographic data can be obtained

EXHIBIT 5–1. GIS DATA LAYERS



from the U.S. Census Bureau for free. This system is called TIGER (Topologically Integrated Geographic Encoding and Referencing). Geographic data can be purchased from third-party vendors that typically enhance this data for improved geocoding. Commercial vendors base the price of the data on its quality and complexity.

2. Focus on ensuring accurate address information. You may need to perform a detailed "cleansing" of the addresses from your CAD/RMS data to ensure quality information within the GIS.

3. Transfer address information from CAD/RMS. An agency can either download the data to a GIS or establish connections to existing databases. The ideal method depends upon the department's current network and CAD configuration.

4. Add a geocoding process. Accurate maps are the essence of a GIS and a process should be put in place to maintain the changes that occur in the area represented by the maps.

Questions To Assess Needs and Configurations

- Does your city or county have a GIS currently in place?
- For what purposes will GIS be used?
- Are there any other departments in your jurisdiction that are using or planning to use GIS?
- Will GIS data be used to support CAD or 911 systems?
- Does your CAD or RMS vendor have a geofile that could be exported for use with your department's GIS solution?
- What is the condition of the agency's address data?
- What steps will need to be taken to provide clean address data to the GIS?
- Will the agency need other software for AVL or parole applications?
- Who will maintain the GIS data?
- Can better address control be obtained from the 911 provider in the form of the master street address guide (MSAG) tape?

Crime Mapping

An agency's RMS and CAD system are used to manage calls for service, assign available units to calls, process critical location information, and track and monitor police-related incidents. Although these systems may provide the ability to conduct ad-hoc queries, the technology to analyze this information and conduct crime analysis has not been available until recently with the introduction of crime mapping application software (generally an extension of GIS software). By combining data from the GIS, RMS, and CAD systems the focus of police work has recently turned to a more data-driven decision-making endeavor.

Crime mapping involves focusing on where crimes happen rather than on just the offenders who commit them. Police agencies are analyzing crime and call-for-service data in an attempt to reduce crime, solve problems, and provide more efficient and effective services to the public they serve. Because of the success of crime mapping efforts and the affordable cost of this technology, many more agencies are incorporating this powerful new tool into their day-to-day operations.

Crime mapping is a tool for crime analysis. The primary objectives of crime analysis are pattern analysis, problem analysis, and operations analysis. We will look at the objectives in detail so you may determine the potential benefits of a crime mapping system for your agency.

Pattern Analysis

Crime mapping is used to identify the spatial and temporal elements of crime patterns and series. Both the geographic pattern and chronological sequence are assessed on a regular basis to develop a profile of who may be responsible for a crime, as well as predict the time of day and day of week for the targeted area. In an attempt to prevent future crime through intervention, the profile is used to apprehend criminals by querying known offender databases and

providing investigative leads. Finally, by correlating the current pattern to similar criminal events, an attempt is made to clear cases and enhance prosecution of habitual offenders.

Problem Analysis

Crime mapping is an instrument for conducting problem solving—known as SARA, or the scanning, analyzing, responding, and assessing of community problems. Crime mapping allows officers to conduct pre- and post-tests of police and community initiatives and measure for the displacement of crime and disorder.

Operations Analysis

Crime mapping also is used to allocate resources, conduct comparative workload analysis, design more efficient schedules, and realign police boundaries. In doing so, officers are in a better position to respond to calls for service and neighborhood concerns in a more timely and effective manner.

State and local governments also can use crime mapping to develop strategic plans. By using a wide variety of geographically referenced information, jurisdictions are looking at risk and protective factors, planning urban renewal projects, and sharing a variety of data across social institutions (schools, police, probation, social services, courts) in which data sharing did not exist before the advent of GIS.

Producing maps that provide visual pictures and reference points for understanding the scope and nature of crime and criminals is the essence of crime mapping. The old adage that a "picture is worth a thousand words" holds true for commanders, line-level personnel, and citizens alike. Using digital maps to display temporal and spatial crime patterns, incorporating symbolization and color, and underlaying an orthophoto adds new understanding to the relationships otherwise not apparent between crime, criminals, victims, targets, and other temporal/spatial dimensions. The beauty of crime mapping and GIS is its flexibility. Massaging the data and producing "what-if scenarios" makes this tool invaluable for decisionmaking and strategic modeling.

Steps for Developing Crime Mapping Capabilities

1. Provide training to a dedicated staff to ensure the crime analysis unit is capable of producing quality products for quick-turnaround requests and regular demands of operational managers.

2. Develop geographic data that includes points, lines, and polygons that represent geographic locations, streets, alleys, bike paths, rivers, lakes, parks, parcels, bars, banks, ATMs, crack houses, sex offender residences, schools, etc. The base map and its peripheral layers of data make up the starting point for any crime mapping system.

3. Provide access to crime data that includes offense, field contacts, traffic citations, accidents, criminals, victims, and arrest information that should normally be stored in the RMS. Costs associated with the crime data are for gaining access by downloading or building database structures or making inquiries to filter data. An agency can either download the data to a dedicated crime mapping database or establish connections to existing network databases. The ideal method depends upon the department's current network and RMS configuration. The crime mapping staff should work closely with the jurisdiction's management information system (MIS) department and CAD/RMS vender to determine the most efficient way to gain access to the crime data.

4. Provide access to imagery data, which includes mug shots, crime scene photos, and floor plans that can be stored as a layer and linked to geographic points. Again, access to this data depends on the agency's current configuration. Some of these systems may be homegrown systems, proprietary systems, or shared regional systems. Access to each computer environment needs to be assessed and solutions tailored to each case.

5. Develop crime maps, which include point symbol maps and thematic maps as seen in the examples in this chapter.

Mapping products that are provided in a timely and regular manner allow for informed decisionmaking and accountability. It is through the ongoing

assessment of community problems and viable strategies that agencies are improving their efficiency and effectiveness in preventing, suppressing, and apprehending criminals, and, thus, improving citizens' quality of life.

Questions To Assess Needs and Configurations

- Is your crime data available in a digital/computer format?
- Does your city or county have a GIS currently in place?
- Are there any other departments in your jurisdiction that are using or planning to use a GIS?
- How dynamic is your jurisdiction, geographically? That is, is your community growing at a fast rate or has growth been stagnant?
- How do you plan to use maps in the course of your operations? Will maps be used to look for patterns, conduct problem solving, allocate resources, deploy troops, or dispatch officers?
- Who will be expected to use the maps? Officers, citizens, managers?
- Who will produce the maps? Officers, analysts, computer staff, clerical staff?
- How will these results be disseminated? Electronically, on paper, via e-mail, over the Web?

What Are the Common Problems and Pitfalls?

- Not having dedicated staff to handle the crime mapping/analysis function.
- Not providing adequate training.
- Not investing in quality base maps.
- Not dealing with data integrity issues.
- Not improving the IT systems that feed a GIS.
- Financial constraints.
- Not addressing the agency's propensity for change.
- Not implementing a process to keep GIS data current.

For more information about crime mapping and analysis, visit the following sites on the Web: the Crime Mapping Research Center, www.crmc.org; the Crime Mapping and Analysis Program, www.nlectc/nlectcrm/cmap.htm; and the International Association of Crime Analysts, www.iaca.org.

Chapter 6. Information System Connectivity

Until now, you have been reviewing and making decisions on application software that is specifically written for the law enforcement world. Some of the approaches are new, but for the most part, the concepts have remained familiar. We are now at the part of the information technology project where the comfort level for many law enforcement personnel changes. *Megabytes? Gigabytes? What is an ethernet LAN? Why are there so many different types of cables?*

You can relax. First, remember that if you are planning a complex system, not only will the software vendor assist you with hardware and connectivity requirements, so will the hardware vendors. If you have hired a network engineer, this person will also have expertise in these areas. This chapter is written for the nontechnical person and covers basic concepts and what your agency will need to evaluate in the area of computer and networking requirements.

Let's get started.

Computer networks allow computers to share information and resources such as printers, disk arrays, backup tape systems, and e-mail, and to gain access to other networks such as the Internet. The network can be as simple as a cable connecting two computers or as complex as thousands of computers connected together, like the Internet. The individual systems must be connected through a pathway called the transmission medium. All systems on the pathway must follow a set of common communications rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules that govern computer communications are called protocols.

Most organizations utilize "special" computers called servers that are used to store information and to manage printers and other common resources. In a typical law enforcement agency, one server would be running software for a CAD system, and another server would be running complementary software for an RMS.

Local Area Network (LAN) Architecture

A LAN is a collection of computers contained in one geographic location and connected directly to the transmission medium, such as cabling. A typical computer network is composed of three functional segments: the servers, the users' computers or workstations, and the LAN infrastructure or transmission medium.

Server

The server is a computer used as a repository for information. Thus, it can be a single point of failure for an entire law enforcement agency. Therefore, it is of utmost importance that the server be built to maximize reliability. To that end, the following is recommended:

- Each server should have redundant internal power supplies and should continue to operate even if a power supply fails. The power supplies should be "hot swappable" so that a failed power supply can be replaced while the server is fully operational.
- The disks should be "hot swappable" so that a failed disk can be replaced while the server is fully operational.
- The power to each server should be protected by an uninterruptable power supply (UPS) and a generator that should be capable of powering the system if commercial power is lost.
- The server should have remote management capabilities so that the support staff is informed of failures and can take appropriate action from a different location, if necessary.

Server Safekeeping Procedures
Servers should be kept in controlled or restricted areas with limited physical access. Resources that are essential for the processing of sensitive data and resources essential to the accomplishment of

organizational missions should be located in these controlled or restricted areas. The operational areas of major computer installations, the server center, and the backup data repository should be designated restricted areas to which access is not permitted, unless specifically authorized or required for job performance.

Controlled and restricted areas should be protected by physical security and other means that are deemed appropriate for the sensitivity or criticality of the system. At a minimum, contract maintenance personnel and others not authorized for unrestricted access but who are required to be in the controlled area, should be escorted by an authorized person in the controlled area.

The disks, tapes, or other media used to record and store sensitive software or data should be labeled, protected, controlled, and secured when not in actual use.

Workstations

Workstations are the end-user interfaces and are usually a Pentium®-based PC (personal computer) running a version of the Microsoft Windows operating system. Due to the fast-paced improvement of PCs, any specifications given here would be outdated by the time this document is published. However, some minimum specifications are a Pentium II 450 MHz processor with 32 megabytes of RAM and a 3-gigabyte or larger hard drive.

Infrastructure

The infrastructure is the most technically complex component of a network. The infrastructure represents how the computers on a network are connected to each other and to the server(s). It also represents how the information itself is carried and manipulated throughout the network. The cabling is know as the *transmission medium.* The information handling is done by *active devices,* such as routers, hubs, and switches.

Cabling

Cabling is the backbone of the network and carries the signals to all the systems connected. The cabling is in twisted pairs and is available in primarily two rating levels: Category 3 (Cat3) and Category 5 (Cat5). Cat5 has a higher data rate capacity. Cat5 cabling has the ability to accommodate data rates up to 100 Mbps (megabytes per second).

One specific type of LAN, called *ethernet,* is currently the dominant networking technology. Its continued success is due in large part to the number of installations, its ability to handle growth (scalability), ease of migration, low inherent cost, and minimal learning curve. A typical ethernet cable transmits 10 Mbps over the cabling. A fast ethernet transmits 100 Mbps over the cabling.

Here are some basic rules and suggestions for ethernet or fast ethernet networks:

- Since the cabling is so crucial to the operation of the entire network and may require specialized equipment to troubleshoot problems, it is important to abide by the specifications of the particular type of cable. If the specifications are not followed, the network performance will not be reliable. The network may begin performing erratically for no apparent reason.
- The maximum number of computers on a LAN is 1,024.
- The cabling should be Cat5 for future capability; however, for existing installations, Cat3 can be used.
- The maximum recommended cable segment length is 100 meters.
- Never use telephone wires for network wiring.
- When purchasing network interface cards (NICs), purchase ones that are capable of handling 10 Mbps and 100 Mbps transmissions; they cost about the same.
- The network protocol of choice TCP/IP (transmission control protocol/Internet protocol), which is the basic communication language or protocol of the Internet and most networks.

For any *new* facilities, a structured cabling system should be designed and installed with Cat5 cabling. The design should meet the requirements of the Electronics Industry Association/Telecommunication Industry Association (EIA/TIA) *568A Commercial Building Telecommunications Standard.* Cabling

outside a building must be electrically isolated, such as fiber optic cabling, or must be attached to commercial services such as the telephone network or cable TV network. Current state-of-the-art facilities usually include a combination of copper and fiber optic cables.

Each work area or office should have a minimum of two information outlet ports, one for voice and one for data. Horizontal cabling (with a maximum length of 100 meters) connects the information outlet to the centrally located communications equipment room. Although the EIA/TIA standard recognizes three media types for horizontal cabling, it is recommended that only Cat5 cabling be used for horizontal runs. According to the EIA/TIA 568A standard, horizontal cable runs are limited to 90 meters; the remaining 10 meters are allowed for work area and telecommunications closet patch and jumper cables. **Never use telephone patch cords for network cabling.** Telephone patch cords may work as network cables, but they will deliver erratic performance.

The communications equipment room should house network equipment, such as hubs, switches, and patch panels, and will probably also contain other telecommunications equipment, such as telephone patch panels, uninterruptible power supplies, etc. **It must have sufficient AC power available and sufficient heating and cooling for the active equipment.**

Active Devices

Active devices handle and manipulate data as it travels across the cabling of a network. Before we explain what the active devices actually do, we must look at the possible ways data can be transmitted over a network. For example, you are sending an incident report from your desktop to the RMS server. The file may be transmitted all at once, in one "packet." In this case, the file has a dedicated cable for transmission. If it is sent all at once, the sending computers must receive an electronic confirmation that all of the information has been received. Otherwise, it will retransmit or repeat sending the file.

The file may also be transmitted by breaking it down into smaller packets of information and sending it with packets from unrelated files. By interspersing the packets, more than one transmission can be made over a cable at the same time. If the file is sent in packets, the sending computer must specify the number of packets and how to put them back together at the other end. The receiving computer has to acknowledge that it received every packet in order and can assemble them correctly.

The active devices used to manipulate the data over the network include hubs, switches, routers, or combinations.

- *Hubs* are inexpensive devices that act as repeaters. As a result of the retransmission of data, they create congestion problems and are recommended for 10 or fewer users. Additionally, according to the ISO standard, only two hubs can be in the path of a data packet.

- *Ethernet switches* are recommended for connecting user workstations and servers. They forward packets only to the appropriate computer based on a packet's actual destination address and are known as intelligent network devices. Thus, an ethernet switch maximizes throughput by reducing traffic congestion. A network may have several switches.

  A small network (exhibit 6–1) would use the core switch for the servers, PCs, and all other equipment. In a large network (exhibit 6–2), the core switch handles information from the servers to smaller switches, called workgroup switches. These workgroup switches, in turn, handle data to PCs, printers, and other peripheral equipment.

- *Routers* are devices that further reduce traffic congestion, but are expensive, complex to configure, and typically induce delays. They are primarily used for connecting to wide area networks (WAN).

Small Ethernet Network

A small network is one that has 1 to 5 servers and fewer than 25 workstations, as shown in exhibit 6–1.

This network can be constructed with one or two ethernet/fast ethernet switches and structured cabling. Recommendations:

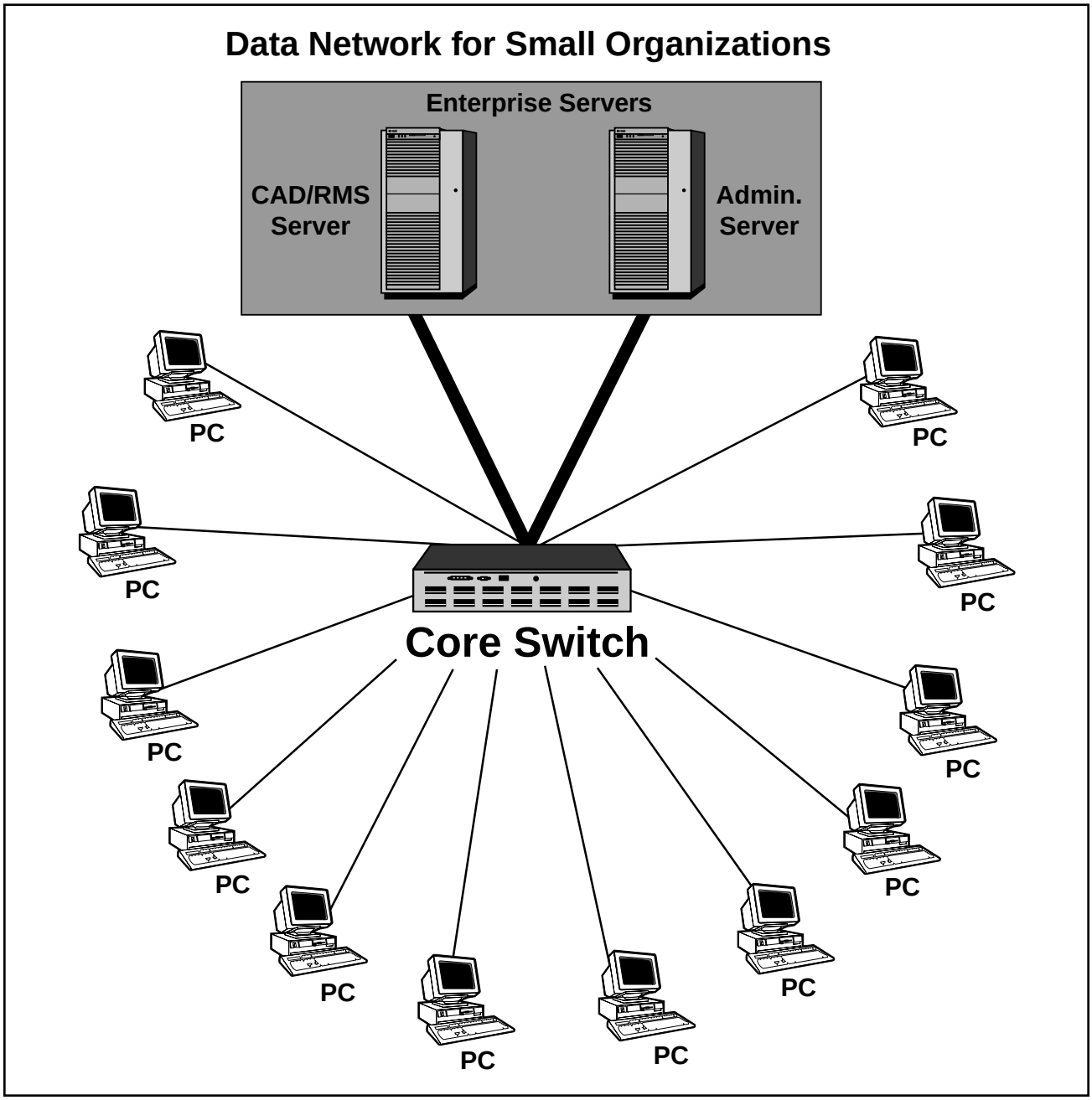
- A fast ethernet switch should be used as the core for the network.

- Enterprise-wide servers should be connected to the network via a 100 Mbps connection on the fast ethernet switch.
- The users should be connected to the network via a 10 Mbps connection on an ethernet switch. While the majority of the switches can be 10 Mbps, the switch needs to have at least one 100 Mbps uplink to connect this switch with the server.
- TCP/IP is the recommended protocol.

Security concerns:

- Without any form of perimeter security such as a firewall,[3] this network should not be connected to any other network either directly or indirectly.

EXHIBIT 6–1. SMALL ETHERNET NETWORK



[3] A firewall is a device that connects two networks and has the ability to examine a data packet to determine source address, destination address, and the type of payload. It is capable of allowing the data to reach the destination network or blocking the data based on a set of rules as defined by the security administrator.

- Without additional authentication techniques beyond user name and password, no dialup modems or workstations with dialup modems should be connected to this network.
- Information on the servers should be backed up regularly and the media should be stored in a fireproof facility away from the communications equipment room in a secure, controlled space.

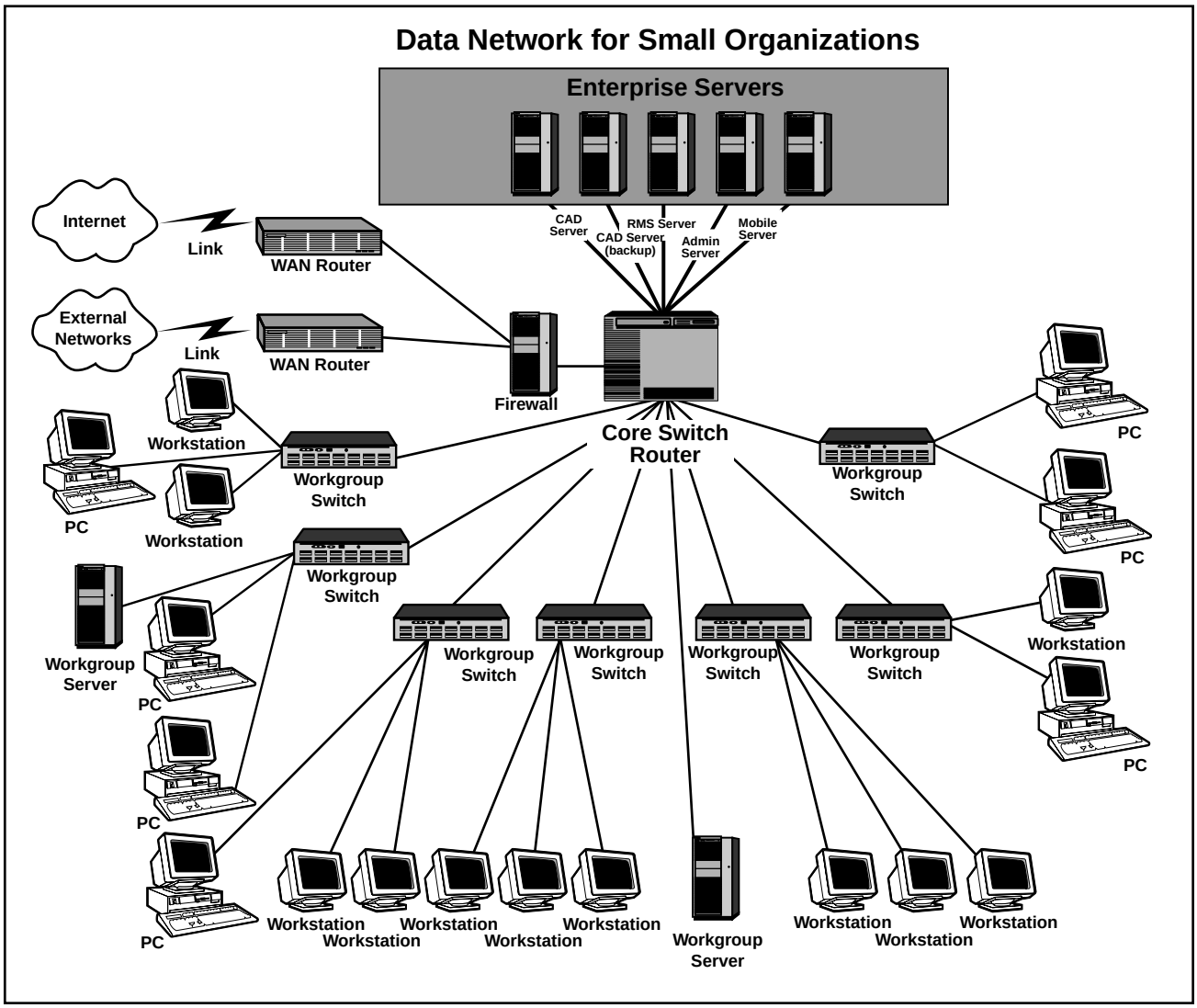
Large Ethernet Networks

A large network is one that has a large number of nodes or connections, such as more than 3 servers and more than 100 PC workstations (exhibit 6–2).

As features are added, the network quickly gets more complicated.

- A fast ethernet switch router should be used as the core for the network.
- Enterprise-wide servers should be connected to the network via a 100 Mbps connection on the fast ethernet switch.
- The users should be connected to the network via a 10 Mbps connection on an ethernet switch. While the majority of the switches can be 10 Mbps, the switch needs to have at least one 100 Mpbs uplink to connect this switch with the fast ethernet core switch.

EXHIBIT 6–2. LARGE ETHERNET NETWORK



How Do I Connect to Other Agencies?

There are many choices for interagency connectivity, but to keep this document to a workable size the scope will be limited to several of the most popular techniques: leasing dedicated links from the telephone company, leasing cables from commercial vendors, using dial-up connections, the Internet, and wireless options.

If the distance between sites is less than a few miles, you may be able to purchase a relatively inexpensive wireless link to connect. These short links may require a Federal Communications Commission (FCC) license for radio-based systems or may require line-of-sight for infrared or optical-based systems. Of course, some of these systems do not operate when something comes between the two sites, such as rain or birds, so check into these short-distance links thoroughly before you buy.

There is no simple solution because there are so many possible ways for longer distance communications. Some of the questions that need to be asked are: How far away is the other agency? How often is there a need to communicate with the other agency? How much data needs to be exchanged? How secure does the link need to be? How much and what level of technical expertise is required for day-to-day maintenance and operation of the solution? Additionally, since you may have no control of the interface at the other agency, you must determine what technique they currently use for interconnecting. We'll take a look at the possibilities for interconnecting over distances.

Dial-Up

Generally, the simplest and cheapest technique for communicating with another agency would be to use a PC that has a dial-up modem and dial into the agency's network. Of course, you will need permission and probably a user ID and password. Since user IDs and passwords are not very secure, the other agency may limit your access to only public information. If this technique is not acceptable for whatever reason, then you will have to sort through the many other possibilities. Your local telephone company can assist you in making some decisions, but remember that it is in business to make money, so proceed with caution.

Direct Links

If the distance between sites is more than a few miles and you need more capacity and security than is provided by a dial-up modem, you will need to contact a public communications carrier such as your telephone company or a long distance provider to lease a point-to-point link. These are capable of data rates exceeding those of dial-up modems and are more secure, since you know where both ends are located. Of course these direct links require more expensive hardware and the monthly cost of the link is dependent on the distance and speed desired. Next, we will discuss the more popular types of direct links.

Asynchronous Transfer Mode (ATM)
ATM is an international standard and is expected to become the dominant transport for all telecommunications carriers. It is the first technology that can deliver different types of traffic (such as voice, video, and data) over a single digital transport mechanism. ATM is connection oriented, and provides quality of service (QOS) by guaranteeing certain traffic types higher priority than others when needed. ATM also can handle scalable amounts of bandwidth, as a result of its switching architecture, which can support multimedia applications and network growth for years to come. ATM has achieved worldwide acceptance and will have a tremendous impact on wide area networks.

Frame Relay
Frame relay provides a packet-switching data communications capability that is used across the interface between user devices (for example, routers, bridges, host machines) and network equipment (for example, switching nodes). As an interface between user and network equipment, Frame relay allows one site to communicate with many sites while requiring only one interface to the network. Current frame relay standards address permanent virtual circuits (PVCs) that are administratively configured and managed in a frame relay network.

Integrated Services Digital Network (ISDN)
ISDN is similar to a dial-up line, except that it is

digital. It is available in two configurations, the basic rate interface (BRI) and the primary rate interface (PRI).

The ISDN BRI service offers two 64k channels and is meant to carry user data. Many systems are able to integrate the two channels to achieve an effective 128 kbps. The cost is approximately $100 per month.

ISDN PRI service offers 23 64k channels yielding a total bit rate of 1.544 Mbps. The cost is approximately $1,200 per month.

Internet Link

The Internet is universally accessible to the public and operates as a confederated network of networks. This technology was designed to provide a standard means of interconnecting networks so that any system could communicate with any other system. However, the ability to communicate does not mean the Internet offers easy connectivity. Interfaces still need to be established to accommodate differences in application software. Also, data on the Internet is sent as plain text, so sensitive data should be encrypted before transmission.

Intranet Link

An intranet is a network that is contained within an agency, designed around Internet technology. The agency usually has geographically distant locations, so the intranet is used as an inexpensive transport for data. The main purpose of an intranet is to share agency information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.

Extranet Link

An extranet is a collaborative network that uses Internet technology to link businesses with their suppliers, customers, or other businesses sharing common goals. It is typically closed to the public (a "closed user group"), but is open to the selected partners.

Companies can use an extranet to:

- Exchange large volumes of data using electronic data interchange (EDI), which is a standard for exchanging various types of business data.
- Share product catalogs exclusively for those "in the trade."
- Collaborate with other companies on joint development efforts.
- Jointly develop and use training programs with other companies.
- Access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks.
- Share news of common interest exclusively with partner companies.

Wide Area Network

A WAN interconnects LANs. The WAN can be located entirely in a local geographic region or may be interconnected around the world. WANs are characterized as being more complex than LANs and the technology is expensive. The choices for connections for a WAN are diverse.

Wireless Communications/ Connectivity

Wireless users should be able to connect to all of the information to which they have access on the agency's LAN. Typically, the wireless data will reach a tower and will be sent over telephone lines back to the agency. The agency will have a device that will sort the data and can route it on the LAN, if necessary. At that point, the wireless users will have access to any of the resources available to them on the LAN. Therefore, if users on the agency's LAN can access RMS or NCIC, they will be able to access these as wireless users.

Other than being able to roam around without a wire connection, the major difference in being a wireless user versus a LAN user is the speed of the link. Data running over a LAN such as an ethernet network is typically 10,000 kbps, whereas the data running over a wireless network is typically at a much lower rate. What does that mean? The data sent over the airwaves will seem very slow compared to the speeds available on the LAN.

We take an indepth look at different types of mobile data communication in the next chapter.

What Type of System Security Measures Do I Need?

How important is information security to a law enforcement agency? To show the importance, let's examine a simple example. Suppose an agency has incriminating information about a case on its RMS. And suppose the suspect is facing possibly spending 20 years in jail. How much would it be worth for the suspect to have this information destroyed or altered? Possibly a few thousand dollars? Or maybe a few hundred thousand dollars? He can hire an entire team of hackers for a few hundred thousand dollars. System security should be of utmost importance to a law enforcement agency.

WARNING: If an information system is connected to other systems or networks, the information system is at risk. No matter how good a password scheme may be, the system is at risk if it is connected to other systems. To borrow an adage, the security of your system is only as strong as its weakest link.

The following are suggestions that can help an agency steer clear of a few blatant security problems:

- A law enforcement network should not be connected to any external network, either directly or indirectly, without some form of perimeter security such as a firewall.
- No dial-up modems or workstations with dialup modems should be connected to a network without additional authentication techniques beyond login name and password.
- Servers should be backed up regularly and the media should be stored in a fireproof, secure, controlled facility away from the computer room.

If a law enforcement agency must connect its system to other networks, it needs a full security system. The first step in building a successful security system is to perform a risk assessment. The risk assessment helps balance the "risks" versus the "cost" of protecting. It also helps stimulate thinking about the likelihood that a security event will occur and the damage that will result if it does occur.

What are some of the possible outcomes if a law enforcement system is compromised?

- Undercover officers and informants can be exposed and placed in danger.
- Confidential information can be disclosed without authorization and the agency can be vulnerable to lawsuits.
- Data can be altered or expunged.
- The system could be inoperable for an extended period of time.
- The agency could suffer a loss in reputation.
- The ability to prosecute offenses could be placed at risk.

What are some of the threats?

- Outside intruders, hackers, and criminals.
- Virus attacks, including Trojan horses and electronic "bombs."
- Insider sabotage.

What needs to be protected?

- Agency personnel.
- Agency data.
- Agency assets such as workstations and servers.
- Agency reputation.

Once the risk assessment has been performed, how can the assets be protected? Security control should prohibit a potential threat or at least limit the impact associated with a threat. Such security falls into three categories: physical controls (previously discussed restricted or controlled areas), administrative controls, and technical controls.

Administrative Security Controls

Based on the risk assessment, the agency should develop a set of written and accepted security policies and procedures that address:

- Acceptable use.
- Unacceptable use.
- Access levels of user accounts, including remote access.
- New employee check-in.
- Exiting employee check-out.
- How data backups are handled.
- How operating system security updates are installed.
- Incident handling procedures.
- Disaster recovery plans.

Technical Security Controls

The internal network should be protected by a firewall and network access should be monitored. Sensitive data should be encrypted before it is transmitted over an open network. Additional levels of authentication should be required for systems that contain sensitive information. External Web servers should be outside the firewall. For example, if your agency has a Web site that is accessible by the public, the Web server would need to be outside the firewall.

Intranet
As mentioned previously, an intranet is designed around Internet technology but is contained within a company, agency, or other enterprise. Since the information that resides on an Intranet is usually confidential or at least sensitive, the data is encrypted before being placed on the Intranet. When received at the remote end, the data is decrypted, thus creating a virtual private network (VPN). Typically, a VPN can be set up between two firewalls of the same manufacturer and will appear to be invisible to the users. Access to an intranet should be open for all users within the company or agency.

Internet
Internal systems should be protected from the Internet with a firewall. The access rules should be set up such that users on the internal network can access anything on the Internet. Valid users attempting to access an internal computer from the Internet should have to pass through the firewall and should be required to use additional authentication techniques, such as dynamic passwords. All other access from the Internet should be denied.

There are many techniques for encrypting information to be sent over any open network. However, the best technique is to create a VPN using the two firewalls.

Extranet
An extranet is typically behind a firewall, just as an intranet usually is, and closed to the public (a "closed user group"), but unlike a pure intranet, it is open to the selected partners. Encryption/decryption via a VPN is an important part in the creation of an extranet.

Wireless
Anyone with a radio can receive wireless data since it is broadcast over the air. Therefore, the only way to secure wireless data is to encrypt it. Cellular digital packet data (CDPD) systems have encryption built in, and the other wireless systems have that option, but it may not be included in the price quoted in a proposal. Therefore, each wireless system will need to be examined to determine which systems are utilizing encryption to protect your data.

We have tried to keep the discussion as nontechnical as possible so you will be better able to understand what is "behind the curtain" in the computer room. As we stated at the beginning of this chapter, you will have help from the software and hardware vendors as to the requirements for your network, and (for a fee) they can usually help with the physical installation.

Chapter 7. Mobile Data Communications

Overview

Mobile data systems installed in police vehicles can increase the effectiveness of the officers by providing timely access to information regarding outstanding warrants and other significant facts. Mobile data can reduce the burden on the dispatch staff and free up valuable voice communications resources by reducing the number of routine inquires generated by officers in the field. The implementation of a mobile data system requires extensive effort by all parties involved.

Mobile data communications systems have relatively low data transfer rates compared to those of a LAN; thus, without a breakthrough in technology, many of the features of the agency's information system are unavailable to the mobile user. For example, some mug shots require 8 minutes to transmit, which is too long for a typical traffic stop. Therefore, much consideration must be given to what is transmitted and what can be loaded on the local mobile computer.

All mobile data communications systems require the same basic infrastructure. This includes radio towers, base stations, base station links, radio network controllers, message switches, radios, and modems. All of the systems can be tied in to the public telephone system, so communications with other agencies is, theoretically, easy. However, the cost of obtaining this type of communications is high. Security of messages can typically be ensured by encrypting them, but discuss this with a prospective vendor, as costs and coverage areas are affected. Of the radio systems available, there are essentially three types for mobile data communications: a traditional private radio system and two commercial systems. Choosing the right data communication services involves three principal decision factors: coverage, capacity, and cost.

Private Radio Systems

Private radio provides a customized radio network that can be constructed for specific private use after obtaining an FCC licensed radio spectrum. Agencies typically select private radio because most commercial services cannot satisfy their needs for coverage and convenience. Cost is the biggest drawback to private radio since the agency purchases the entire infrastructure. The agency absorbs the entire cost of constructing the system, which can be millions of dollars. Coverage for private radio is limited primarily due to build-out costs. To make private radio economically feasible, users typically must be concentrated in a relatively small area.

Private radio systems can be constructed utilizing 800 MHz trunking radios or the standard 150 MHz radio frequencies (RF). It is highly recommended that an agency utilize different channels for voice and data communications, so two complete systems are required. Over the years many agencies have moved their voice communications to 800 MHz trunking and are no longer using certain RF channels. These RF channels can be used for mobile data communications. However, some RF systems are not capable of data transfer rates at 9600 Baud or above, so be sure to check with a vendor to determine the maximum data rates that are available.

Commercial Systems

Wireless telephone companies offer commercial services such as the circuit-switched cellular and packet radio systems. By utilizing a commercial system, an agency is able to obtain mobile data communications by paying a monthly fee for service and purchasing the vehicle-related equipment. However, these systems are shared systems and the agency has little control over important decisions such as capacity planning and prioritization. There are also concerns in the public safety community that shared services may not be available during a disaster because of the increased demand due to influx of the news media and the issue that public safety has no specifically designated priority. The two most common commercial systems are circuit-switched cellular systems and packet radio systems.

Circuit-Switched Cellular Systems
Many wireless telephone companies offer circuit-switched systems. These systems can transmit a continuous stream of data using the standard analog or digital voice cellular channels. Modems are added to convert data for transmission over the standard voice channel. Circuit-switched systems provide the greatest capacity of any of the existing cellular systems because data can be transmitted at a greater rate. The primary drawback to these systems is cost. Since data is transmitted over the analog voice channels, cellular carriers typically charge comparable rates to voice service (monthly charge plus a per-minute usage rate). Circuit-switched systems are best used for large file transfer, faxes, and Internet access.

Due to the all-digital nature of PCS (personal communication service), data connectivity could be less complicated. Some PCS telephones have a built-in modem that permits a direct connection of a computer to the cellular handset with just an interface cable.

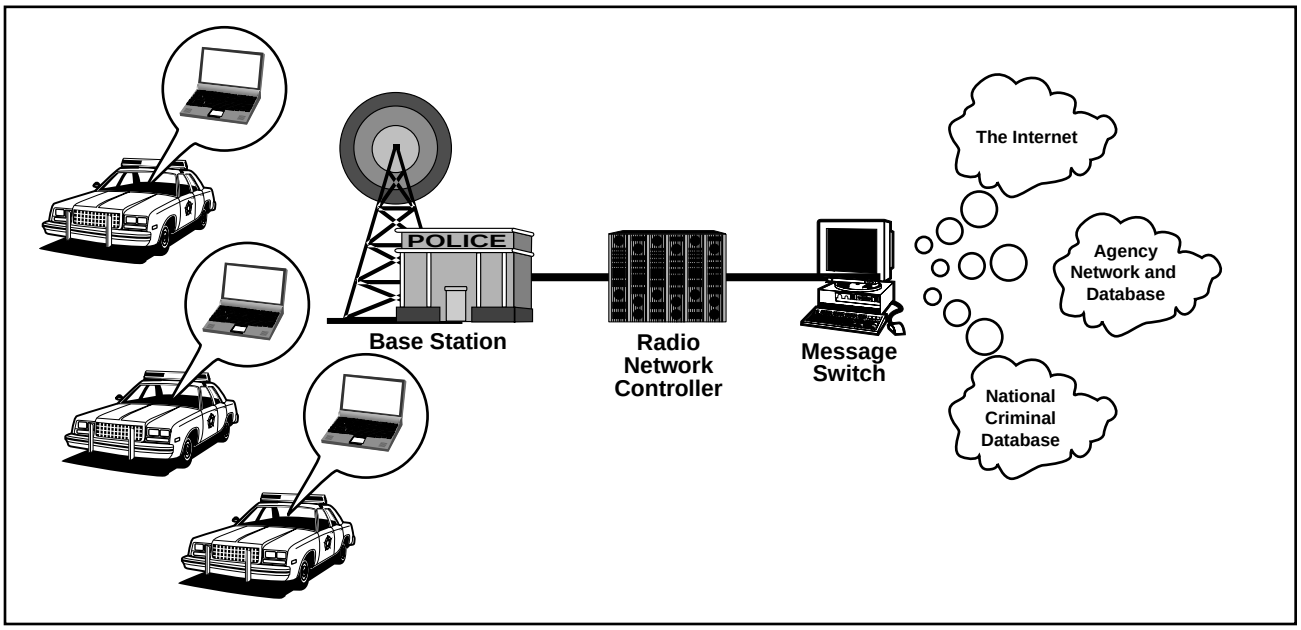
Packet Radio Systems
Packet radio systems break the data stream into smaller packets for transmission over wireless channels. As a result, a large number of users can share a given network by interlacing the packets of data.[4] With packet-switched networks, packet transmissions are generally conducted in bursts and are not constantly being sent out. This type of operation permits the base station's modem to receive packets interspersed from many users and to correctly reassemble the many different messages. Implementation costs can be higher because packet radio requires either modification to existing cellular systems or build-out of a new infrastructure. Coverage is usually limited to metropolitan areas only, which can be a major drawback for extensive systems. In general, packet radio is best used for frequent person-to-person data communication such as e-mail or route management services.

Equipment Components

One of the major components of a mobile data system is the infrastructure required to support the RF portion of the system. This infrastructure includes the radio repeaters, antennas, modems, network controllers, and other associated site equipment. This equipment is used to receive, transmit, and control the RF portion of the system and to provide an interface from RF to data. Whether a system is traditional private radio, circuit-switched cellular, or packet radio, the infrastructure building blocks are very similar.

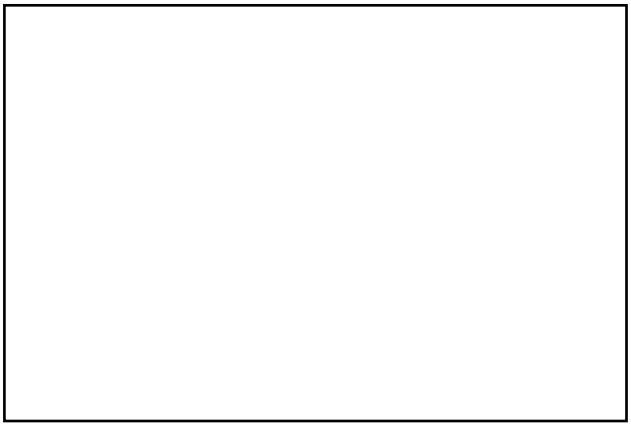
The necessary hardware elements for data communications over a mobile link are shown in exhibits 7–1 and 7–2.

EXHIBIT 7–1. HARDWARE FOR A MOBILE DATA NETWORK



[4] *Packet-switched vs. Circuit-switched*, Bell South, 1997.

EXHIBIT 7–2. VEHICLE HARDWARE FOR A MOBILE DATA NETWORK



By utilizing a commercial wireless provider, the user needs to be concerned with only coverage, capacity, usage fees, and disaster planning, but not the cost of building the infrastructure. The commercial provider should be able to produce a coverage map indicating which areas are accessible and the expected transmission rates.

Exhibit 7–2 displays the equipment necessary to equip a vehicle for mobile data communication. The choice of cellular telephone or radio depends on the choice of transmission systems. A private radio system and packet radio system would require a radio; whereas, a circuit-switched system requires a cellular telephone. For either system, the receiver/transmitter must have the ability to accept an interface from a personal computer such as a modem. The type of modem used will depend upon the choice of computer and the transmission system. If a standard laptop computer is used, it should have at least one type III PCMCIA card slot. The manufacturer or a third party should be able to provide an interface cable.

Technical Assessment

Before approaching a commercial system provider or a private network vendor, the working group should determine the present-day needs and expectations and should attempt to predict the future needs and desires. They should perform a detailed analysis of other radio and mobile systems to help guide the expectations. The detailed analysis should include:

- Physical measurements.
  - System coverage.
  - Data capacities.
  - Environment (indoor/outdoor, high/low temperatures, day/night).
- System considerations.
  - Specifics of the existing infrastructure.
  - Expected growth.
  - Types of data being communicated, now and in the future.
  - Interfaces required to connect to other systems.
  - Problems experienced with the current system.
  - Determination of procedures that are dependent on the system.
  - Determination of procedures that need to be changed to efficiently operate with the new system.
  - Type of security required.
  - Transmission of messages in plain text versus encrypted.

Physical Measurements

System Coverage

Existing radio system coverage should be mapped against the geographical considerations of the agency. Coverage measurements should include the required range of signal strengths. Lapses in the current system coverage may or may not be considered to be significant to overall agency operations. For instance, coverage may not be required in the middle of a large lake. Any lapses in coverage that affect agency operations should be reflected in user interviews or during the measurement process and taken into consideration when designing a new system.

Coverage prediction software can be used to help select site locations and identify potential areas of insufficient coverage. Remote sites may be colocated with existing public safety communications sites, and the need to duplicate building, power, and telecommunication assets will be minimized.

Data Capacities
Perform an analysis of the potential loading of the system. The factors that should be included are (1) peak number of active users, (2) number of inbound and outbound messages per hour per terminal, (3) size of the messages, (4) turn-on times for base and mobile stations, (5) potential system delays, and (6) coverage reliability. Users of the system need to be aware that large files such as mug shots or fingerprints will require large amounts of system resources. If this type of usage is anticipated, it must be clearly stated in the RFP. The percentage a channel is actually in use for specific periods during the day is important to understand user needs. For instance, a "spike" in usage around 7:30 a.m. due to roll call may mark an operational consideration. Also, the percentage of calls blocked due to channel congestion could help justify the need for additional channels. The vendor selected to construct the system may also perform a similar survey of the data loading, and the results can be compared. Additionally, the data being transmitted via radio should use some method of encryption so that unauthorized persons cannot easily intercept the data.

System Considerations

The mobile data system selected should consist of multiple remote sites. All transmitters used at the remote sites should be capable of continuous operation with sufficient power output. The transmitters should be able to provide full-power output in a very short time, usually 10 milliseconds or less, and be able to withstand frequent on-and-off switching cycles. Receivers at the remote sites should be designed specifically for data reception and should be capable of measuring and reporting incoming signal strength. Ideally, the system should be configured so that the loss of one of the remote sites will not prevent the remainder of the system from operating.

Mobile radios used in the system should be designed for data service and should be easily interfaced to a modem. A single system controller device should keep track of activity on the system and provide control of the remote sites. The controller device can use cellular, trunking, or frequency reuse technology, but should be capable of dynamically reassigning system assets to make maximum use of the remote sites. Normally, the system controller device will be located at one of the public safety dispatch facilities, and communication with the remote sites can be made by microwave or leased wireline. The system controller device should also be capable of performing some network functions and data conversions. Data from the controller device will flow to a message switch for distribution to the various users.

Analytical Models

Based on system traffic loading and coverage, models and simulations could be developed to more completely define current system performance. These models can be used during the technical assessment. Geographic information systems are very helpful in displaying data graphically. GIS data can include both analytical results and physical measurements.

Factors Affecting Performance

In a wireless environment, there are many factors that can affect how well a mobile data system will work. Unlike a fixed network environment in which external influences can be minimized, wireless networks have far more variables that can reduce performance.

Stationary
In a motionless situation, the two most prevalent factors that can affect data transmission are short-term fading and multipath. Fading is the result of signal variations caused by terrain, buildings, and path loss if the transceiver is out of range of a base station. Multipath is caused by reception of multiple copies of the same signal arriving at different levels or times and is common in either a stationary or dynamic environment. Multipath and fading contribute to errors in digital data communications that result in reduced performance.

Dynamic
When a transceiver is in motion, many factors can degrade performance. In addition to the static problems encountered in signal propagation, the dynamic environment is influenced by:

- Fading from nearby structures, both moving and fixed.
- Signal variations due to terrain.

- Coverage problems in fringe areas.
- Radio frequency interference from other sources.
- Path loss from foliage.

Other
Factors outside the RF environment that can degrade mobile data performance include problems that can occur within the network itself. Some examples are:

- Data resends due to misconnection of the sending and receiving units.
- Packet delays or drops.
- Congestion from large numbers of users or other network delays.

End-User Queries

The success of mobile computing depends on it meeting the needs of the end users. The end-user community should have been defined during the technical assessment. Results of interviews with end users should be taken into consideration when defining the future needs of an agency.

As technology advances, the equipment for mobile data communications can transmit or receive a greater amount of data than possible just a few years ago. However, choosing the best alternative for the type of system your agency needs depends on cost, coverage, and expected use. Taking the time to explore all options is key to choosing a mobile data communications system.

Chapter 8. Request for Proposal Development and System Selection

Your procurement objective should be to hold a fair competition, making sure that the process results in the selection of the best vendor without protests from the unsuccessful bidders. This chapter discusses the development and issuance of an RFP and system selection, steps 10 and 11 from the project plan introduced in chapter 2.

You will need to assemble a team to develop and evaluate an RFP. This team most likely will be formed from members of the working group you established to review your agency's processes. Again, you will need one person to be in charge of the project, so it is best to establish a project manager for the RFP development, evaluation, and implementation.

RFP Development

Acquisition of a system can be achieved with minimized risk through the development of an RFP document that will tell potential vendors:

- Your objectives and current conditions.
- What you want to buy.
- How you want to buy it.
- How you want vendors to structure their proposals.
- How you will evaluate their responses.

Local government policies permitting, an RFP can take on any form you like as long as it is easy to follow. Before we proceed to the details of an RFP, there are a couple of important points that can maximize your success. If you are buying a complex system, it will cost each of your vendors time and money to develop a proposal. It is therefore incumbent upon you to develop an understandable document. Each vendor will review your RFP and either formally or informally go through a "bid/no bid" decision based upon their probability of capturing the job. The more complex the system, the smaller the vendor pool. In order to maximize the number of responses to your RFP, you might want to consider one of a few different methods to let your vendors know your intentions and ask for their opinions. Vendor feedback will be critical when you start to write your RFP. One more very important point: If you do not select a winner after evaluating all responses, it is almost impossible to get vendors to rebid on a modified RFP. In this situation, vendors will believe you do not know what you want and this situation might continue through the implementation phase, an environment that can be risky for all parties.

Structure

Most RFPs are organized into the following major sections:

1. A cover letter.
2. An introduction and summary section.
3. Proposal preparation instructions (PPI), evaluation criteria, and vendor qualifications section.
4. A Statement of Work (SOW) section.
5. A system specifications section.
6. Amplifying appendixes.
7. A sample contract.

There are no set formats to an RFP. Some agencies have refined their RFP processes and have a format that everyone uses. The important thing is to have all the necessary content and to put it in a logical order. With the advent of the Internet, some agencies have been publishing their RFPs on the Internet so that vendors can read and respond. Also, some organizations have developed a service to publish RFPs and notify subscribing vendors of RFP publication. You can use these sources to study RFP construction and content for system purchases that are similar. Keep in mind, there is no free lunch; you should review someone else's work very carefully before adopting it as your own. A good Web site to

visit for sample RFPs and similar documents is www.search.org.

Cover Letter
The cover letter usually introduces the project, summarizes the intent of the effort, and informs prospective bidders of important dates and responsibilities. The head of the agency typically signs this letter.

Introduction
The introduction usually includes:

- A description of the project objectives.
- Due date for the proposal (usually 45 to 60 days after the RFP release date).
- The environment in which the system will operate.
- System sizing parameters such as message volumes or number of records to store.
- Critical interfaces.
- Conversion of legacy records from older application software systems.
- End-to-end system response goals.
- Jurisdictional demographics, including predicted growth (if necessary).
- Implementation timelines.

Proposal Preparation Instructions
This section tells vendors how their responses are to be organized. It is important that all respondents organize their responses in a like manner. When the time comes to evaluate these responses, this is your only way to compare "apples with apples." The most common types of responses are usually broken down into three parts: What the vendor will do (Technical Volume), how the vendor will manage the work (Management Volume), and what it will cost (Cost Volume). When a municipality buys an easily defined and specified item like a street or sidewalk, the municipality can easily control the risk of failure and, therefore, make the job award based on cost. The same usually is not true for complex purchases such as IT systems. In these cases technological approach and management expertise usually are more important to mitigate risk. Evaluating the technology and management volumes first, and then modifying scoring based upon cost factors generally yields the most successful purchase of a complex IT system. In many cases, the same people who evaluate the technology and management approaches do not do the evaluation of cost. Therefore, it is common practice to have the vendor's cost volume bound separately. A typical PPI can address any and all of the following topics:

- The maximum number of pages each volume may contain.
- Page layouts, including line spacing, font sizes, and margins.
- Templates for costing summaries and specification requirement matrixes.
- Organization of the vendors' responses.
- Compliance statements or forms.
- Financial statements.
- Qualifications of key personnel.

You probably will not know everything to include. For example, the purchasing department may require compliance statements regarding indemnifying insurance and completion bonds. This is where you turn to your newfound friend in purchasing and ask that he or she supply you with this information.

The best way to ensure the vendor responds to your RFP with information you want to evaluate is to publish the method you will use to evaluate the responses. This is called the evaluation criteria. By publishing these criteria in your RFP, you also can mitigate the problem of award protests by losing vendors. These criteria are usually made up of major categories and list the amount of weight that will be assigned to each category. Some sample evaluation categories might be:

- Project understanding.
- Design risk.
- Management methodology.
- Experience and qualifications.
- Vendor plans such as implementation, testing, or cutover.

- Project cost, financial risk, or cost realism.

For example, if you assign the project cost as 10 percent of the evaluation grade, the vendor can infer that cost is not the driver in your purchase, but it can be a decisionmaker for two competing and equal proposals.

If this task sounds overwhelming, take heart. In one form or another, the PPI has been prepared thousands of times before and you can use someone else's example as a starting point. A checklist of possible items for inclusion in the PPI is included in the appendix.

Statement of Work
This is the section in which you tell prospective vendors what you want them to do and where they derive the cost. To successfully implement your project, not only will you be buying delivered and installed pieces of hardware and software, you also will be buying:

- Vendor project management.
- System spare parts.
- System acceptance testing.
- System maintenance and warranties.
- Training.
- Documentation.

This is the section in which you detail how you will manage the vendor to mitigate risk. For example, you will require the vendor to supply and maintain project schedules and plans, as well as participate in periodic formal reviews of progress made. This is the most important section in your document, and if carefully thought through, one of the easiest to write. It is important to note that this is the only place you can detail how you control your vendor(s) and your project implementation.

System Specifications
The bad news is that system specifications can be difficult to write; the good news is that you've done most of the work with your as-is and to-be maps. You can use the to-be maps to show the overall flow of information. The notes you have made to accompany the maps can be the starting point of the written specifications. These specifications should be written to include the level of detail recommended in chapters 4 and 5.

One important point to remember is the specifications never state how many things you want, only what the pieces must do. Unless it is a requirement, do not specify products by brand name. You will find that as you edit this section you will be removing these types of statements. Six simple instructions for developing requirements are that they should[5]:

- Only specify external system behavior.
- Specify constraints on the implementation.
- Be easy to change.
- Serve as a reference tool for system maintainers.
- Record forethought about the life cycle of the system.
- Characterize acceptable responses to undesired events.

When purchasing a complex system it is easier to manage and describe your requirements if you break your system down into a set of subsystems and then detail the requirements for each subsystem and how each subsystem interfaces with other subsystems. For example, if you were buying a mobile data computer (MDC) system for police cruisers, you might break it down into an in-auto subsystem, an in-station message switch subsystem, and a dispatch display subsystem. You would then detail the specifications for each subsystem and its interface requirements with other subsystems or existing outside systems. When writing the specifications, try to be as complete as necessary but avoid the level of detail that would result in only one product meeting the need. When you get involved with the evaluation of various technologies, vendors will be quick to offer product descriptions with specifications for these products. Understand that a vendor's specifications may be written to drive you toward its product.

---

[5] K.L. Heninger, *Specifying Software Requirements for Complex Systems,* 1980.

You will also need to provide vendors with the response criteria to ensure a consistent response method and fair evaluation. The following example instructs vendors to indicate at what level their products will meet each specification. Specifically, it requires vendors to state whether proposed software is part of the standard package or if customized software will need to be written. The evaluation process is made easier with this level of detail in the response. This type of response provides you with a clear picture of what you are getting for your money and helps you to understand where additional money might need to be spent to get exactly the system you want.

This section contains response documents that must be completed and submitted with the proposal. Failure to complete and return these sections of the RFP will be a basis for disqualification. These sections are to be returned on the original form provided. In no case shall requirements be retyped or altered in any way from those provided within. The RFP will not be provided electronically.

Each item in these sections must be marked with one of the following "status codes":

[A] Requirement is included and may be demonstrated in the proposed software package.

[B] Requirement will be provided by proposed modifications to the base software package in the price proposed.

[C] Requirement will be provided by a standard option. The cost of these options must be provided in the cost section of the proposal, with reference to the RFP section and function.

[D] Requirement will be provided by new custom software programming. The cost of the modification must be provided in the cost section of the proposal, with reference to the RFP section and function.

[E] Requirement not being proposed.

In the event that additional information is to be provided to further describe the method in which the proposed system meets the specific requirement, a plus (+) must be entered to the left of the status code box on the response form, sub as +[B].

A proposal section that addresses each requirement identified with a plus (+) must be included following the response forms. Each requirement being addressed must be identified by RFP section number and function. Those items marked with and asterisk to the right of the status code box ([ ]*) are mandatory requirements.

The vendors will use the response criteria to respond to each item of the specifications. An example of specifications follows:

Respond to Calls for Service

[ ] The system should create an event record when a call comes into the agency.

[ ] The system should automatically insert automatic number identification/automatic location identification (ANI/ALI) information into the event record.

[ ] ANI/ALI display information should be formatted identically to and contain all information provided by the telephone company.

[ ] ANI/ALI information should include zone service providers for fire, EMS, and police.

- [ ] The system should automatically insert administrative line caller identification information into the event record.
- [ ] The system should be able to process multiple dispatch configurations, single agency, multiple departments (fire, EMS), or multiple jurisdictions.
- [ ] The system should allow entry of sets of questions to provide the dispatcher with online questions to ask of the caller, based on the type of incident.
- [ ] The system should be configurable to allow multiple offense code tables based on agency or jurisdiction.
- [ ] The system should provide the capability to select event type from a list and automatically insert the selection into the field.
- [ ] The dispatcher should be able to select calls by priority, time, or specific call.
- [ ] The dispatcher should be able to suspend one call to take another of higher priority.
- [ ] The dispatcher should have the ability to queue calls.
- [ ] The system should clearly indicate an in-process call.
- [ ] The event should be able to be transferred to another call taker for completion at any time during the entry process.
- [ ] The system should automatically route the event to the dispatcher responsible for the location entered.
- [ ] The dispatcher should be able to interrupt and suspend an event that is being entered in order to service an event, which has a higher urgency.
- [ ] If an event is entered which is later determined to be a duplicate of another event, the dispatcher should be able to cancel the event and have it permanently cross-referenced by the primary event.
- [ ] Each event record should be logged based on a unique system-assigned event number based on agency or jurisdiction.
- [ ] When the responding officer requests an incident number, the system should assign a unique case number based on the agency's numbering scheme.
- [ ] Event records should not be required to have a corresponding case number.
- [ ] The dispatcher should have the capability to verify and correct, if necessary, the caller name, phone number, and address captured by E911 while preserving the E911 information.
- [ ] Data included for an event record should be the caller information, address of event, event code, officer assigned, and dates and times of call.
- [ ] Call priority levels should be configurable within the system based on the agency's policy.
- [ ] Incoming calls should be automatically prioritized for dispatch based on the type of call.
- [ ] The dispatcher should have the capability to override the priority level set by the system.
- [ ] The system should provide automatic capture of time of call, time of dispatch, time of arrival, and time of departure and/or a configurable method for times to be collected.
- [ ] The dispatcher should be able to supplement, modify, and cancel incidents after entry into the CAD system.
- [ ] An automatic search of names, addresses, driver's licenses, or vehicle licenses should be performed when entered into the system.

- [ ] The system should provide the capability to associate "Alert" data to a name or an address for hazardous materials, Be On the Lookout (BOLO), warrants, missing persons, medical alerts, vacant houses, residential and business burglar alarms, pistol permits, and orders of protection/restraining orders.
- [ ] The system should automatically check for and be able to display "Alert" data based on the name/address search of the RMS for hazardous materials, BOLO, warrants, missing persons, medical alerts, vacant houses, residential and business burglar alarms, pistol permits, and orders of protection/restraining orders.
- [ ] The system should allow multiple "Alert" records to be entered for a single location.
- [ ] The system should include a geographic file for address verification and event mapping.
- [ ] The system should identify nearest cross streets, streets on either side of an address, and the jurisdiction.
- [ ] The system should be able to display a map of events associated to a name and address (or within a two-block area) within a defined period of time.
- [ ] The system should be able to display geographical zone maps indicating call-for-service locations and identify police units.
- [ ] The system should allow assignment of location types, e.g., residential, business, government, etc.
- [ ] The system should provide alerts for officers on duty who have not checked in in a defined time period.
- [ ] The system should support to-do lists for officer tasks such as address checks, and should provide automatic time stamping when an officer indicates a task is performed.
- [ ] The system should support standard dispatch as well as call-taker dispatch configurations.
- [ ] The system should provide accountability for on-duty personnel.
- [ ] The system should allow for the entry of calls that have been previously handled but not yet entered into the system, due to conditions such as system unavailability.

The system specification could include additional sections for all external agencies that would use the systems being proposed. Therefore, it is imperative to understand these agencies' systems, especially the current operating environment, the communications operations, and the average daily volume of calls.

In summary, organize this section with care and, where possible, include diagrams and design drawings to amplify your written statements.

Appendixes
The last section is typically a set of appendixes that provide amplifying information. Items in this section can include:

- A sample contract.
- Template tables and forms.
- Acronym definitions.
- Applicable floor plans of affected areas.

After your draft RFP has been modified, edited by the stakeholders, and approved for release, it's time to pull out your list of qualified vendors and send your RFP out. This concludes what is called the preproposal phase of your project.

RFP Release

You should mail your RFP to a particular person within a vendor's organization and follow up with a telephone call to confirm receipt. Recently, some agencies have been publishing their RFPs on the Internet to increase exposure. The good news with this method is that you will have much exposure;

the bad news is that you will not have a clue as to who is going to bid unless you have prospective vendors register their intentions. Unless your procurement is extremely complex, a typical schedule would be:

1. RFP release.
2. Bidders' conference 1 week after the RFP is received by the vendors.
3. Written Q&A for an additional 2 weeks.

Once you release the RFP, expect the vendors to have questions. You will need to plan the way in which you respond to the questions. At a minimum, you will want to establish a single point of contact within your agency to handle the questions-and-answers process. You will also want to conduct a bidders' conference. Both are discussed below.

Questions and Answers

The vendors should never be allowed to talk to anyone other than the established point of contact within your agency. Whatever information is given to one vendor must be given to all other participating vendors in writing. You should accept written questions from vendors for a defined period of time, and the questions and the responses should be sent to all prospective vendors in writing. If the playing field is not maintained level during this phase, the whole competition may be at risk. Your whole team should understand this point and the vendors must understand that they can be eliminated from the competition for violating this rule.

You will have to get guidance from your procurement attorney about how you publish the questions and answers. Some agencies state in their answers which bidder asked a question; some do not. If your policy is to state which vendor asked a question and the vendor pool knows this, certain vendors will not ask questions during the bidders' conference (see below). Knowledge of which vendor asks a question can be as valuable to competitive vendors as the question itself is.

Make sure to keep good records of all questions and answers as well as to whom you sent responses. Note: You may receive written questions before the bidders' conference. In these instances, you can go into the conference with prepared answers. Some agencies place a statement in their RFP cover letter allowing for this occurrence.

Bidders' Conference

After the RFP has been received and reviewed by the vendors, the next step is to hold a bidders' conference. Depending upon the complexity of the project, you can decide to make this optional or mandatory. As an example, if the new system has to interface with other existing systems and there are physical placement issues, you might want to make this mandatory. However, if the purchased item is a software upgrade, it may not be necessary to make the conference mandatory.

The purpose of this conference is to describe the system you need, allow the vendors to ask questions about your RFP, and provide facility tours, if necessary. Providing a verbal description of your needs at the conference may seem repetitive of your RFP, but the face-to-face meeting will add information and help clarify your written document. Try to have the whole presentation made by the program manager, but have everyone who contributed to the RFP in attendance to help with the answers to questions. Ensure that you make an audio recording of the entire proceedings.

You should not feel that every question posed at the bidders' conference must be answered on the spot. However, within a week after the conference, provide written answers to all questions to all prospective vendors. At the conclusion of the conference have each vendor identify a single point of contact as the recipient of written responses.

Proposal Evaluation

During the period that follows the Q&A/bidders' conference and the receipt of the proposals, you should spend your time preparing for the evaluation of the proposals.

In order to hold a fair competition and minimize the risk of protests, prepare an evaluation process in writing and then follow it. Typically, your RFP has detailed the criteria you will use to evaluate bids. However, it is critical to ensure the evaluation criteria and process is set prior to viewing the responses.

Further, ensure you can produce documentation to this effect if required to demonstrate your RFP process as a fair and competitive one.

Evaluation Team Selection

Select an evaluation team that is able to evaluate all subjects of the bids. Your team does not have to include your working group (chapter 2) or RFP development team, although, in most cases, some of these people will be on your team. Generally, the project manager you have assigned to develop the RFP will continue to manage the evaluation portion of the RFP. You can have team members who are called to evaluate only certain sections of the bids. For example, if a complex procurement included a radio subsystem, you might have communications people evaluate just that section of the bids.

During the evaluation process, ensure that the evaluators have no conflicting assignments. The best way to handle this is to do your evaluation away from any work areas. If possible, select an offsite or at least an insulated location. It is important to have the undivided attention of the evaluators while they are working for you.

Evaluation Procedures

Step 1
Whoever is in charge of the evaluation process should read all proposals and set aside all nonconforming bids. A proposal can be considered nonconforming if it does not:

1. Offer to sell everything you want to buy.
2. Offer to sell the system to you in the manner you want to buy it.
3. Respond in the format you requested.
4. Deliver the system to your schedule.

If none of the responses conform, it probably means your procurement or RFP is not constructed well—it is either too vague or too specific.

Step 2
Convene your evaluation team and start by providing the team with a review of the system to be procured and the major provisions of the RFP. Summarize the proposals to be studied and tell the team about proposals that will not be evaluated and why. Establish a rule that no proposals can be removed from the evaluation site and that no discussions about the proposals should occur with anyone away from the site. Inform your team that you have technical help available to explain complex issues and provide any team member with a tutorial on a technical matter associated with the procurement. Tell them that they will be evaluating the technical and management volumes first and that the cost volumes will be evaluated later. Based on the complexity of the system and the evaluation criteria, you may select special individuals to only evaluate the cost volume and factor their scoring into your decision. Prepare and distribute to your team a matrix of the system specifications and vendor responses by vendor. This will provide the team with a comparison of each vendor's software and a good method for determining which vendor can match the most requirements. The evaluation team should prioritize which requirements are most important to the agency.

Step 3
Using prepared evaluation forms, have members of your team evaluate the management and technical volume on their own, at their own pace. After everyone finishes their evaluations, you may want to consider a group discussion in which evaluators describe their scoring. You can allow evaluators to modify the scores based on these group discussions.

During the evaluation of complex responses, some agencies will evaluate all proposals and then select a smaller set of proposals for a final, very detailed evaluation. In these instances, an evaluation may include a presentation and a Q&A session with "finalists."

Products of the Process

The evaluation team now develops a recommendation of a system and an associated cost, but generally does not have the authority for the actual procurement. This authorization rests with someone in senior management. It is the project manager's job to take the results of the evaluation team and present them to this authority for a decision. You should also organize and retain the written evaluations of each member of the evaluation team. In certain instances the selecting authority may ask to see this data or

ask you how the team evaluated a particular vendor. If the contract award is protested by any of the vendors, having this information well organized will be very helpful.

Contract Award

In some municipalities, counties, and States, statutes may restrict price and terms negotiations prior to a contract award. In those cases, the process is almost mechanical and is handled by the procuring entity. In some cases, municipalities, counties, and States may allow for negotiation with the vendor or possible vendors for a best and final price and terms. In these cases, you may be called on to help in these steps and in the final selection between competing finalists. The most important point to remember is that this step is the job of the procuring entity and you may have to provide advice. Your RFP may have detailed the type of contract to be awarded, such as fixed price, cost plus a fee, and/or incentives base on performance or schedule. One of the negotiating possibilities would be a switch in the type of contract to use. In this case, you should be ready to advise your procurement entity of the benefits and shortfalls of this approach. It is important to understand that unless negotiated out of an agreement, your RFP will state that the vendor's proposal becomes part of the contract document. In these cases, there usually is an RFP statement that lists the order of importance of each document that is part of the contract.

A payment schedule must be worked out prior to contract award. This is your opportunity to limit the risks associated with the procurement. Work with your procuring agency to develop a payment schedule that does not let the payment of funds get ahead of system installation. For example, you might try to withhold payment of certain funds until a critical technology piece is installed and working. It is your job to advise your procuring agency on how to tailor payments to minimize risk. If you are concerned about your ability to do this, have the vendors include a payment schedule in their proposal and have them explain and justify their schedule of payments.

As you work through the process of developing an RFP and evaluating the responses, you can get help for almost all facets of these tasks, but it will be up to you to provide the common sense, intuition, and leadership to make your project successful. The same holds true for the next steps in the process, "installation management and beyond."

Chapter 9. Installation Management and Beyond

This chapter describes the implementation and maintenance of the selected system. This is the final step in the project plan presented in chapter 2. This step is an ongoing process. Once a system is installed, you must keep your eyes open to ways to use the system more efficiently and to indications that an upgrade is needed.

If you have done your RFP correctly, the SOW will give you the vendor controls you need to manage the implementation phase of the project. Aside from the items you want to buy, the SOW should give you the control you need over the vendor to ensure a timely implementation with minimum risk. This is accomplished by requiring the vendor to keep you informed of project schedules and by establishing a review, reporting, and approval process at various steps along the way. No matter how well you have done your RFP, no matter how well the vendor's design is, things may change before the system is up and running. Your ability to identify these instances early will determine how well you control the schedule and cost changes for your project. Either you or an assigned person must stay on top of the project, notice problems quickly, and be prepared to act quickly to these instances.

Project and Vendor Management

Project Schedule

Vendors should present a preliminary copy of their project schedule as part of their proposals. Aside from the opportunity to evaluate these submissions, you can make the winning vendor's schedule the starting point for the implementation phase. You should then require the vendor to keep this schedule current throughout the implementation phase of the project. This product can be a very valuable tool when you are providing project status information to your management.

Customer Responsibilities

You will be responsible for providing an acceptable location and environment for any equipment that will be installed during the implementation. The vendor should give you information concerning what is required that should address issues such as electrical power requirements, air conditioning, and space requirements. You will be responsible for ensuring that the location will be ready early enough to meet the schedule. You will also be responsible for ensuring that the network cabling is in place to accommodate the new system. Consider how you want the system to function if there is a disruption of commercial power. Decide if an uninterruptible power supply is sufficient or if a backup generator also needed. This equipment should be installed in sufficient time to accommodate the vendor's schedule.

Project Reviews

It is a good idea to require the vendor to present a project review at certain logical times during the implementation phase. This review should include a presentation of the project design if it has changed from the proposal, or if the SOW required the development of a design as one of the project deliverables. The review should detail the updated project schedule, status, and anticipated problems that have to be solved. This review provides an opportunity to invite your project stakeholders, members of other internal departments, senior management, and any other interested parties. You should have the vendor put together an agenda for your approval before this event and ensure this event is structured and focused. The number and spacing for these reviews will depend on the project complexity. If you do not know enough about the number of reviews to hold when you prepare the SOW, you can have the vendor propose a review schedule in their proposal.

Progress Reports

The vendor should report on the status of the project in writing on an established periodic basis.

Obviously, this product can be sent to various people for their study. Most importantly, if the project experiences some problems, these documents will become part of any legal discussions with the vendor about performance. Ensure the SOW spells out the form and content of these reports.

Project Costs

Certain projects will involve a cost that is dependent on the amount of services or products delivered. An example might be a project in which you hire a company to develop a software program and the vendor is under contract to provide programmers at a negotiated hourly rate. In some circumstances either you or the vendor must track expenses and provide this information against a project budget. If the vendor is tracking costs, this information can be added to the project reviews and progress reports.

Plan Approvals

A valuable aid in maintaining control of the project is to have the vendor prepare various plans that must be approved prior to implementation. These plans can include:

- An overall project plan.
- A management plan.
- An implementation plan.
- Testing plans.
- Training plans.
- Cutover plans.

As mentioned above, you can make sure of these plans as part of the vendor's proposal and evaluate them as an indication of project understanding. The plans fall into two categories: (1) static plans, which are prepared once and approved prior to execution, and (2) changeable plans, which are constantly updated and made part of the review process. By injecting yourself into the approval process for static plans, you maintain a level of project control and are in a position to define steps the vendor should take that may not have been obvious prior to the start of the project. Static plans such as testing or training plans typically are submitted by the vendor at some defined period prior to their proposed implementation and must be approved by you prior to their execution.

Documentation

Have the vendor provide you with documentation of the system and the work that was done. The type and complexity will depend on the project. Types of documents can include:

- Manuals for off-the-shelf supplied items.
- Manuals for vendor-developed items.
- Drawings of the finished system (as-built drawings).
- Testing results.
- Final reports.

Most of these items are self-explanatory. One item that you should pay close attention to is the documentation for supplied and/or developed software. As a system consumer, you will need to ensure that software changes can be accomplished even if the vendor goes out of business. Therefore, you either need a copy of the software source code and the development environment, or these items must be placed in escrow by the vendor with a condition that these items are turned over to you if the vendor goes out of business. Place this condition in your RFP so that your vendor can price the cost of this requirement.

Acceptance

As previously mentioned, it is a good practice to establish a payment schedule so those sufficient funds are not disbursed until the system is accepted. You will have to develop an acceptance process based upon the delivered system. Acceptance testing by the agency should be spelled out in the RFP. You, the customer, need to take charge of the acceptance testing because you are assuming responsibility for this system. As a result, you need to thoroughly test it and know what features do and do not function correctly. Once you accept the system, the vendor can walk away with your money and has no obligation to make anything else work. So be sure you know what you are accepting. By the time you are ready to accept the product, you should have been trained and should be able to operate all aspects of the system. The vendor might be able to demonstrate the system to you, but you are going to have

to demonstrate it to the rest of the agency. You must demonstrate that all proposed parts and services are delivered, that the system is operational, and that the system performs at the level stated in your system specification. You would not buy a car without test driving it, and would walk away from a car if the dealer would not let you drive it.

System Transition

Unless the purchased system is a stand-alone piece of new technology, your project work is not done until the system is integrated into your agency. If this system is replacing an existing, operational system, you will have to develop a plan and process to switch from the older system to the new one. Switching operations from the old system to the new system is referred to as the *cutover or system transition.*

It is likely that you have purchased new software and hardware. Having new hardware will give you a great advantage as it will allow the new system to be built without having to destroy the existing system. Your vendor will have the ability to set up the new system and perform some testing on your network without taking down your existing system. This will also allow you to bring the old system back online quickly if the new system does not perform quite as expected. This will give you the opportunity to make corrections to the new system without the rush of having the facility down.

You and the vendor should develop a cutover plan that defines how and when the cutover will occur. The vendor's plan should include a fallback plan in the event that unexpected problems occur. Prior to your acceptance of this plan, have this plan reviewed by all the system stakeholders. Unless there is a compelling reason, the transition should occur over time, allowing you and the vendor to work out any glitches.

For example, if you are installing a complex RMS with mobile data terminals, you could bring the RMS server online with access provided to LAN-based workstations. Once you are comfortable that the new RMS server is performing correctly, you could add the reporting function, which would allow personnel to enter followup reports online. Once you verify that the reporting module is performing correctly, you could add some legacy data from the old RMS. Finally, you could tackle adding the mobile data users. If you use this technique and space out the transition one module at a time, you know where to look if problems arise.

Once the entire new system is online, keep the old system in place for a week or two, in case the new system has some cutover glitches and goes down. Modern computer systems have become much more reliable than their mainframe ancestors have, but there is a window of time when a "brand new" computer is susceptible to catastrophic failures due to improper configuration or faulty internal hardware. Keeping the old system in place and turned off for a few weeks should protect you from the vulnerability of having no operational system.

Legacy Data Migration

IT systems require additional work involving the migration of data from the older system to the newer. If the data on the older system is of an unknown form, you will have to plan and budget for the vendor of that system to be involved in the migration process. In most instances, it is legally necessary to convert or migrate the existing data to the new system, or run parallel systems for a substantial period of time. Generally, there are two methods of legacy data migration: (1) migration to the new active databases and (2) flat file transfer.

Migration to the new active databases provides the most comprehensive implementation, enabling all of the data handling capabilities of the new system in dealing with all information, legacy or new. This is usually the most expensive type of migration, since the legacy data must be cleansed and massaged to meet the requirements of the new system. There will be exceptions and issues of noncompliance that will have to be dealt with, and you will need to make decisions on how to proceed as problems are discovered with the data. Bear in mind that actual migration of the legacy data may demonstrate another level of expertise of the vendor, particularly for situations in which the vendor may make substantial updates to the product to keep abreast of technology, requiring a migration from the older version to the newer version. For example, moving from DOS-based systems to Windows-based systems.

While flat file conversion is generally the less expensive of the options, an obvious selling point, there are other considerations. Flat file conversion simply takes existing data from the databases in which it is stored and places it all in one large database. The information is accessible, but cannot be searched in the same manner as new data entered into the new system. In short, the data exists, but two operations will be required for each name search instead of one. The vendor may be able to provide an index link for name searches, but there can be no alteration of the old data (such as entering case dispositions). Additionally, searches other than names are not usually available. Another consideration is how the new system operates "under load." Some vendors may recommend flat file migration because their system, as proposed, will not provide the required response times with 200,000 records already entered. This is a serious consideration, due to the fact that, without legacy data migration, you will not know that this problem exists until well after the vendor has been paid.

It will be up to you to decide how best to migrate your data. In determining the cost of the migration, be sure to include manpower to "clean up" existing data so that it matches, as closely as possible, the data sets required in the new system, the vendor's work in actually massaging and loading the data, and manpower required to check the vendor's work and accept the migration.

Cost of Ownership

In calculating the cost of owning a system, you should consider not just the cost of acquisition, but the cost of maintenance, repairs, and upgrades from system startup until system elimination. It is important when evaluating competing systems or designs to consider these life cycle costs in your evaluation process. You are not expected to be a wizard and conjure these items. You can get a good indication of these costs by asking the prospective vendor to optionally propose maintenance costs for the years after the system goes out of warranty. This should give you a good idea of the near-term costs. The long-term cost is best estimated after talking to people who have similar systems in operation.

Be sure that the maintenance costs include hardware maintenance with your desired response times and software maintenance with software updates. Depending on your level of expertise, you will probably want telephone support so you can call the vendor when questions arise. In addition to the vendor maintenance, purchase some of the high-failure spare parts such as power supplies and disk drives. Having these items on hand should give you a much improved response time in the event of a failure. Two items that are often overlooked are head cleaner tapes and backup tapes (budget enough for a year's worth of data).

If you feel that life cycle cost is a determining factor in system selection, have the vendor provide an estimate of life cycle system costs and make this information part of your evaluation criteria. If this is a brand new system or technology, you will have to revert to best estimates. Again, you can have the prospective vendors provide these estimates in their proposal submission.

Some of the cost factors to consider in calculating the lifetime cost of ownership are:

- Maintenance.
- System upgrades.
- System repairs.
- Subsystem replacements.
- Training.

Appendix. Proposal Preparation Instruction Checklist

The following is a proposal preparation instruction (PPI) checklist of subjects/clauses you may want to consider for inclusion within an RFP. Although the location of these clauses may vary from agency to agency, they have been lumped under PPI. In certain instances, your procurement or contracts personnel will provided these clauses or subjects to you. However, it is a good idea to be familiar with these items because you may have to decide on clause content. Further, you may be the person to enforce these conditions.

General Clauses

- Deadline for proposal submission and submission address.
- Project director.
- Procurement officer.
- Location of work.
- Minimum qualifications.
- Project budget.
- Agency not responsible for proposal preparation cost.
- Disclosure of proposal contents.
- Proposal amendments.
- Protest of RFP.
- Notice of intent to respond.
- Bidder RFP questions.
- RFP amendments.
- Amendment or withdrawal of proposals.
- Supplemental terms and conditions in proposals.
- Discussions with bidders.
- (State/county/municipality) bidders' preferences.
- Assistance to bidders with disabilities.
- Criminal background checks for vendor's personnel.
- Right to inspect offeror's place of business.
- Right of rejection.
- Protest of award.
- Contract negotiations.
- Failure to negotiate.
- Extension of proposal due date.
- Taxes.
- Tax clearances.
- Out-of-State bidders.
- Opening of proposals.
- Bidders request for exceptions.
- State or local debarment.
- Conditional proposals.
- Anticompetitive practices.
- Omissions.

Proposal Format

- Number of copies to submit.
- Minimum font size/line spacing.
- Page limits on technical and/or management volumes.
- Cost volume bid sheets.
- Compliance matrix.
- Delivery instructions.

Contract Information

- Contract type.
- Contract term.
- Contract approval.
- Standard contract provisions.
- Insurance requirements.
- Bond requirements.
- License requirements.
- RFP is part of the contract.
- Proposal is part of the contract.
- Additional terms and conditions.
- Substitution of vendor personnel.
- Contract changes.
- Funding.
- Payments.
- Unacceptable deliverables (quality of goods).
- Termination for default.
- Termination for convenience.
- Ownership of documents.
- Assignments.
- Disputes.
- Severability.
- Unauthorized communications with contracting officer.
- Waiver of informalities.
- Contract award.
- Cancellation of award.
- Statutory or ordinance requirements.
- Sexual harassment policy for bidders.

Law Enforcement and Corrections Technology Advisory Council

Chair: Carl R. Baker
Vice Chair: Martin F. Horn
Vice Chair: Kenneth Bayless

Francisco J. Alarcon
Deputy Secretary
Florida Department of Juvenile Justice
Tallahassee, Florida

Col. Carl R. Baker
Chief of Police
Chesterfield County Police Department
Chesterfield, Virginia

Jim T. Barbee
Correctional Programs Specialist
Jails Division
National Institute of Corrections
Longmont, Colorado

Chief Kenneth Bayless
Field Operations Region III
Los Angeles County Sheriff's Department
Monterey Park, California

Capt. Bob Beach
Commander
Reston District Station
Fairfax County Police Department
Fairfax, Virginia

Simon J. Beardsley
Technology Review Coordinator
Texas Department of Criminal Justice
Huntsville, Texas

John W. Bizzack, Ph.D.
Commissioner
Department of Criminal Justice Training
Richmond, Kentucky

Joseph P. Bonino
Commanding Officer
Jail Division
Los Angeles Police Department
Los Angeles, California

James Brock
Director
Southeastern Public Safety Institute
St. Petersburg, Florida

Bob Brown
Chief
National Institute of Corrections Academy
Longmont, Colorado

G.C. "Buck" Buchanan
Sheriff
Yavapai County Sheriff's Office
Prescott, Arizona

Sam Cabral (represented by Dave Nulton)
President
International Union of Police Associations
AFL–CIO
Alexandria, Virginia

Chief Robert E. Cansler
Concord Police Department
Concord, North Carolina

Nick Cartwright
Director
Explosive Detection Systems Implementation Program
Transport Canada
Ottawa, Ontario
Canada

Steve Chianesi
Assistant Director
Rhode Island Judicial Systems and Sciences
Rhode Island Supreme Court
The Rhode Island Traffic Tribunal
Providence, Rhode Island

Chief Merino Ciccone
Rome Police Department
Rome, New York

Brian Coleman, OBE
Director
Police Scientific Development Branch
Woodcock Hill, Sandridge
St. Albans, United Kingdom

Larry Cothran
Executive Officer
California Department of Corrections
Technology Transfer Committee
Sacramento, California

Chief Gregory G. Cowart
Millbrae Police Department
Millbrae, California

David R. Crist
Warden
Minnesota Department of Corrections
Bayport, Minnesota

Steven F. Cumoletti
Staff Inspector
New York State Police
Planning and Research Section
Albany, New York

Patrick J. Devlin
Assistant Chief
Criminal Justice Bureau
New York City Police Department
New York, New York

Lt. Kirk DiLorenzo
St. Louis Park Police Department
St. Louis Park, Minnesota

Chief Lee Doehring
Leavenworth Police Department
Leavenworth, Kansas

Chris Donnellan
Legislative Director
International Brotherhood of Police Officers
Alexandria, Virginia

George Drake
Region Manager
Adult Probation and Parole Division
New Mexico Corrections Department
Albuquerque, New Mexico

Chief Richard D. Easley
Kansas City, Missouri, Police Department
Kansas City, Missouri

Chief Richard Emerson
Chula Vista Police Department
Chula Vista, California

Chief Joseph G. Estey
Hartford Police Department
White River Junction, Vermont

Chief Charlie Fannon
Wasilla Police Department
Wasilla, Alaska

James Fortner
Administrative Lieutenant
Tennessee Department of Correction
Nashville, Tennessee

Sheriff Charles Foti
Orleans Parish Criminal Sheriff's Office
New Orleans, Louisiana

Wendell M. "Pete" France
Assistant Warden
Baltimore Central Booking and Intake Center
Baltimore, Maryland

Steve Gaffigan
Sr. Executive Director
Quality Assurance
Metropolitan Police Department
Washington, D.C.

Gilbert Gallegos
National President
Fraternal Order of Police
Albuquerque, New Mexico

Doreen Geiger
Assistant to the Secretary for Facility Siting and Policy
Washington State Department of Corrections
Olympia, Washington

James A. Gondles, Jr.
Executive Director
American Correctional Association
Lanham, Maryland

Chief Reuben M. Greenberg
Charleston Police Department
Charleston, South Carolina

Mel Grieshaber
Legislative Director
Michigan Corrections Organization/SEIU
Lansing, Michigan

Chief Timothy Grimmond
El Segundo Police Department
El Segundo, California

Capt. Mike Grossman
Los Angeles County Sheriff's Department
Monterey Park, California

Robert Guy
Director
Division of Adult Probation and Parole
North Carolina Department of Correction
Raleigh, North Carolina

Earl Hardy
Highway Safety Specialist
National Highway Traffic Safety Administration
Washington, D.C.

Ben Hathcock
Supervisory Special Agent
FBI Academy
Firearms Training Unit
Quantico, Virginia

Lt. Sid Heal
Los Angeles Sheriffs Department
Special Projects Technology Exploration
Monterey Park, California

Jaime Herrera
Idaho State Department of Corrections
Security Coordinator
Boise, Idaho

Joan Higgins
Assistant Commissioner
Office of Detention and Deportation
Immigration and Naturalization Service
Washington, D.C.

Chief James E. Hill
Port Authority Transit Police Department
Camden, New Jersey

F. M. Hite
Manager
Operations and Training
Virginia Department of Corrections
Roanoke, Virginia

Irving Hodnett
Chief Engineer
FBI Engineering Research Facility
Quantico, Virginia

Chief Stanley Hook
Smyrna Police Department
Smyrna, Georgia

Martin F. Horn
Secretary of Corrections
Department of Corrections
Camp Hill, Pennsylvania

Capt. Geoffrey C. Hunter
Metro Transit Police Department
Washington Metropolitan Area Transit Authority
Washington, D.C.

Stephen Ingley
Executive Director
American Jail Association
Hagerstown, Maryland

Maris Jaunakais
Head
Forensic Sciences Division
Naval Criminal Investigative Service
Washington, D.C.

Jim Jones
Executive Assistant to the Director
Virginia Department of Corrections
Richmond, Virginia

Sheriff Aaron D. Kennard
Salt Lake County Sheriff's Department
Salt Lake City, Utah

Chief R. Gil Kerlikowske
Seattle Police Department
Seattle, Washington

Andrew Keyser
Chief Information Officer
Pennsylvania Department of Corrections
Camp Hill, Pennsylvania

Paul Kirby
Division of Corrections
Charleston, West Virginia

James Klein
Houston Police Department
Inspection Division
Houston, Texas

Chief Robert E. Langston
U.S. Park Police
Washington, D.C.

Henry Lee, M.D.
Chief of Forensic Services
Connecticut State Police-Scientific Services Division
Meridan, Connecticut

Calvin Lightfoot
Warden
Allegheny County Jail
Pittsburgh, Pennsylvania

Kevin Lothridge
Director of Strategic Development
National Forensic Science Technology Center
Largo, Florida

Chief Rodney M. Maggard
Hazard Police Department
Hazard, Kentucky

James Mahan
Senior Technologist
Office of Security Technology
Federal Bureau of Prisons
Washington, D.C.

Michael T. Maloney
Commissioner
Massachusetts Department of Corrections
Milford, Massachusetts

John McCalla
Assistant Division Chief
U.S. Secret Service
Technical Security Division P&D
Washington, D.C.

Edward McDonough, M.D.
Deputy Chief Medical Examiner
Office of the Chief Medical Examiner
Farmington, Connecticut

Harlin McEwen-(R)
Ithaca, New York

Col. David B. Mitchell
Maryland State Police
Pikesville, Maryland

Ron Morell
Training Administrator
Vermont Criminal Justice Training Council
Pittsford, Vermont

Roger L. Payne
Deputy Chief
New Mexico State Police
Santa Fe, New Mexico

John J. Pennella
Director
Applied Technology Division
U.S. Customs
Washington, D.C.

Charles S. Petty, M.D.
Transplant Services
University of Texas
Southwestern Medical Center
Dallas, Texas

Dimitria D. Pope
Assistant to the Executive Director
Community Justice Assistance Division
Texas Department of Criminal Justice
Austin, Texas

Sgt. John S. Powell
Communications Coordinator
University of California Police Department
Berkeley, California

Janet Quist
Business Director
Public Technology Inc.
Washington, D.C.

Rex J. Rakow
Director
University of Notre Dame Campus Police
Notre Dame, Indiana

Col. Michael D. Robinson
Michigan State Police
East Lansing, Michigan

Chief Thomas J. Roche
Gates Police Department
Rochester, New York

Daniel N. Rosenblatt
Executive Director
International Association of Chiefs of Police
Alexandria, Virginia

Tibby Roth
Chief Inspector
Special Technologies Officer
Research and Development Division
Israel Police
Tel-Aviv Jaffa
Israel

Raul Russi
Commissioner
City of New York Department of Probation
Brooklyn, New York

Charles L. Ryan
Deputy Director of Prison Operations
Arizona Department of Corrections
Phoenix, Arizona

Stephen Schroffel
Director
Technology Development
U.S. Immigration and Naturalization Service
Washington, D.C.

Wayne Scott
Executive Director
Texas Department of Criminal Justice
Huntsville, Texas

Lawrence Seligman
Chief, Tribal Police
Tohono O'odham Nation Police
Sells, Arizona

Charles E. Simmons
Secretary
Kansas Department of Corrections
Topeka, Kansas

Capt. Kathryn Stevens
Allen County Sheriff's Department
Fort Wayne, Indiana

Terry Stewart
Director
Arizona Department of Corrections
Phoenix, Arizona

Brad Stimson
National Research Council of Canada
ICPET
Ottawa, Ontario
Canada

Richard Stroker
General Counsel
South Carolina Department of Corrections
Columbia, South Carolina

George M. Taft, Jr.
Director
Alaska Department of Public Safety
Scientific Crime Detection Laboratory
Anchorage, Alaska

Morris Thigpen
Director
National Institute of Corrections
Washington, D.C.

Corp. David Thomas
Montgomery County Police Department
Domestic Violence Unit
Rockville, Maryland

Dennis Tucker
Fleet Manager
Illinois State Police
Springfield, Illinois

Richard Turner
Director
Vermont Department of Corrections/Correctional Services
Waterbury, Vermont

James Upchurch
Chief
Bureau of Security Operations
Florida Department of Corrections
Tallahassee, Florida

Judith Uphoff
Director
Wyoming Department of Corrections
Cheyenne, Wyoming

Gerald D. Weinzatl
Assistant Superintendent
Milwaukee County House of Corrections
Franklin, Wisconsin

Carl A. Wicklund
Executive Director
American Probation and Parole Association
Lexington, Kentucky

Reginald A. Wilkinson, Ed.D.
Director
Ohio Department of Rehabilitation and Correction
Columbus, Ohio

David Williams
Deputy Superintendent for Correctional Services
Coxsackie Correctional Facility
West Coxsackie, New York

National Law Enforcement and Corrections Technology Center
P.O. Box 1160
Rockville, MD 20849-1160

PRESORTED STANDARD
U.S. POSTAGE PAID
JESSUP, MD
PERMIT NO. 4030