Executive Summary

This chapter on Records Management Systems (RMS) is designed to bring together, in one place, technological information and terminology that a chief law enforcement administrator can use, no matter what phase of planning, development or implementation the RMS might be in at the time of reading this document.

The TTAP Advisory Committee and staff designed the TDR to focus on the areas of greatest impact and importance to law enforcement. Because of the critical importance and value of RMS, this section was selected as one of five major topics in the TDR.

The chapter begins by addressing how RMS works and what an RMS consists of. Recognizing that a RMS is not just a means to electronically collect and store reports and information, it holds the core components which a chief will rely on to be informed and make sound and intelligent administrative decisions.

The benefits of a modern RMS to a police agency and its community are realized by its contribution to operational efficiency and resource management. A RMS provides timely and accurate information within the organization through access to information connectivity. Likewise, the RMS provides management with the tools and resources to lead the agency well while maximizing tax payer's dollars.

Developing and implementing a complete law enforcement RMS requires a major commitment from the police agency budget. The section on estimating costs will examine how to take steps to plan for and select the right RMS for an agency.

Challenges to RMS implementation will arise based on the kind of RMS an agency acquires. A successful implementation is made possible by avoiding common mistakes. Some typical mistakes addressed include:

- Trying to implement portions of a RMS before crafting a well-defined program
- Believing an off-the-shelf package alone can be a universal RMS solution that meets all needs
- Attempting to use personnel who don't have records management training or experience to lead the effort

Things to consider, outlines preparation steps for RMS purchase and lists essential components of RMS software. Other sections include identification of needed general functions the RMS system must possess and what performance criteria the system must meet.
The next steps to consider when undertaking a RMS project are purchasing guidelines and specifications for the system. Included in this chapter are the most recent RMS guidelines developed by the IACP, Law Enforcement Information Technology Standards Council (LEITSC) subcommittee on Information Systems.

A sample policy for establishing a RMS program in a law enforcement agency as well as a sample technology press release is included in the chapter.

No major technology initiative could or should be implemented without giving considerable thought to training. The chief must mandate training where technology, especially RMS, is being implemented within the agency. This chapter addresses this important and often forgotten area.

A section on backup systems is an important contribution to this chapter. A sound business plan must be developed to mitigate system failure due to any individual system disruption.
One of the major challenges facing police administrators is choosing the appropriate RMS for their department. A RMS is a major investment that can enhance the services you provide to your community. This records management acquisition can also become a never ending source of frustration which, if not remedied, can lead to poor work production, morale issues and litigation. Listed below are guidelines for a department contemplating the purchase of a new RMS:

- Contact police departments comparable in size, population base, demographics, and location. Ask their administrators what is working for them. Don’t reinvent the wheel.
- Complete a needs analysis. Your department will have specific needs.
- Ensure that the new system or upgrade will interface with your existing system and is capable of interfacing with other law enforcement systems for information sharing. A new system that requires manual transferring of files is not time or cost efficient.
- Inquire about and establish guidelines for attaining technical support. Make sure it is available 24/7, 365.
- Compare pricing. If it appears too good to be true, it is. Some service providers will assist you in securing funding, i.e. grants or donations.
- Look at the history of the contractor. Determine how long have they been in business, their expertise in law enforcement records management, and how many systems they have provided. A company that specializes in law enforcement is usually the best option.
- Make sure the provider designates a specific customer service representative to as a point of contact for your department. This way you will have someone familiar with your department who can readily remedy your problems.

To ensure a successful purchase, do your homework and know that you are providing your employees with the tools to win!

Chief Bill Dial
Whitefish Police Department—Montana
A functional RMS can help prevent, reduce and control crime, improve community policing and problem solving capabilities as well as improve operational efficiency and resource management. The department and community benefit from the improved capabilities and efficiencies that RMS has to offer. Communities are safer because policing agencies are able to do their jobs better through the shared capacities of RMS.

A Guide for Applying Information Technology in Law Enforcement, March 2001
http://www.nlectc.org

The benefits to a department are similar to what a chief would expect as objectives/outcomes once an RMS has been acquired and implemented.

Examples of these benefits are:

- Improving the accuracy and reliability of information within the agency by consolidating departmental records
- Reducing the cost of data entry by eliminating duplication of effort
- Providing a consistent chain of reporting and analysis
- Expanding the use of the system departmentally by providing a system that is easy to learn and use
- Minimizing data handling

A well designed filing system includes the following elements:

- Must make filing less difficult, tedious, and unattractive
- Must offer quick and easy filing and retrieval of information with a minimum of wasted time and effort (e.g., 30 second retrieval time
- Must ensure integrity and continuity of record keeping despite changes in office personnel
- Must have uniform practice
- Must allow for the easy identification and purging of inactive record
- Should provide clear and simple file categories
- Should be expandable and flexible enough to meet everyone's needs
Higher Productivity, Lower Costs

Higher productivity and lower costs are the main benefits of good file management. The right filing system produces important tangible results and eliminates costs associated with poor procedures.

**Time Savings**
- Faster filing and retrieval of information
- Fewer misfiles
- Higher staff efficiency and productivity

**Cost Savings**
- Less frequent purchase of filing equipment and supplies
- Less office space used for filing equipment
- Less time spent on filing
- Less likelihood of litigation losses resulting from lost documents
- Less likelihood of lost documents leading to unfavorable audit findings and penalties
- Less costly recovery of vital records

**Specific Benefits:**
Establishing and maintaining control over files will bring specific benefits such as the following:
- Easier training of new personnel
- Expandability and flexibility to meet the needs of the office
- Standard procedures for disposal of obsolete records
- Improved service to clients/public
- Protection of vital records
- Compliance with legal and audit retention requirements

Adapted with permission from *A Guide for Applying Information Technology in Law Enforcement* by the National Law Enforcement and Corrections Technology Center, 2001. Further reproduction without express written permission is strictly prohibited.

[http://www.nlectc.org](http://www.nlectc.org)
How RMS Works

Source: Law Enforcement Tech Guide

A modern RMS links different data types from multiple users. This allows for the retrieval of that information for strategic, tactical, investigative and administrative uses. The specifics of that information are more particularly described in the LEITSC Functional Standards Guide to RMS located in the appendix of this resource.

The different data types include but are not limited to reports, images, photos, master name indexes, evidence and property information, crime mapping, and computer aided dispatch integration. RMS allows the consumer of the information to look at all available, related and pertinent data on a given suspect, address, phone number, etc. with the purpose of making sound decisions based on that integrated information.

Adapted from the LEITSC Functional Standards Guide, 2006
http://www.leitsc.org

A RMS is an agency-wide system that provides for the storage, retrieval, retention, manipulations, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations.

RMS covers the entire life span of records development, from initial generation until the process to which it is relevant is complete. An effective RMS allows single entry of data while supporting multiple reporting mechanisms.

For the purposes of this document, the RMS is limited to records directly related to law enforcement operations. Such records include incident and accident reports, arrest, citations, warrants, case management, field contacts, and other operations oriented records. The RMS does not address the general business functions of law enforcement agency such as budget, finance, payroll, purchasing and human resources functions. However, because of operational needs such as duty roster, law enforcement personnel records are included. The same is true for fleet maintenance.

This document addresses the following business functions:
- Calls for Service
- Incident Reporting
- Investigative Case Management
In addition, the following support functions are addressed:

- Master Indices
- Interfaces
- RMS System Administration
- RMS Reports

The RMS should provide the capabilities for users to generate inquiries of internal and external data sources, such as the agency's state DMV and criminal history files, as well as NCIC, from within each module where such inquiries make sense.

In addition, the RMS should provide the user with the ability to reuse and/or import data returned from external sources in order to eliminate redundant data entry.

The RMS should also provide the capability to electronically forward RMS data to external data sources either automatically or upon request of the user based upon agency rules embedded within the RMS.

The above capabilities should be based upon established criminal justice standards including: the Global Justice XML Data Model (Global JXDM), the National Information Exchange Model (NIEM), and the National Institute of Science and Technology (NIST) standards including the Electronic Fingerprint Transmission Specification (EFTS), facial recognition collection standards, etc.

Adapted from the U. S. Department of Justice, Office of Community Oriented Policing Services, Law Enforcement Tech Guide, 2002. Text used with permission from SEARCH. Further reproduction without express written permission is strictly prohibited.

http://www.search.org
Due to new compliance regulations and statutes beginning in 2005, records management has gained new interest among corporations. While government, legal, and healthcare entities have a strong, historical records management discipline, general record-keeping of corporate records has been poorly standardized and implemented. In addition, scandals such as the Enron/Andersen scandal, and more recently records-related mishaps at Morgan Stanley, have renewed interest in corporate records compliance, litigation preparedness, and issues. Statutes such as the Sarbanes-Oxley Act have created new concerns among corporate “compliance officers” that result in more standardization of records management practices within an organization.

Privacy, data protection, and identity theft have become issues of interest for law enforcement as well. The role of the RMS to aid in the protection of an organization’s records has often grown to include attention to these concerns. The need for individual record security has brought greater focus to records retention schedules and records destruction.

Used with permission by Wikipedia – The Free Encyclopedia
http://www.wikipedia.org

A RMS is a computer program (or set of programs) used to track and store records. The term is distinguished from imaging and document management systems that specialize in paper capture and document management respectively. RMS commonly provide specialized security and auditing functionalities tailored to the needs of records managers.

Purchase of records management software that will assist with organizing and tracking records could be a worthwhile investment for a local government. Records management software may be developed and marketed by private companies, or may be developed by a local government utilizing a commercially available database management software package and then distributed to other local governments either for free or for a small fee.

Governments interested in purchasing records management software often do not have a clear idea of the capabilities of such software, nor do they know where to begin their search. Specific software requirements will vary by size and type of government.
Before purchasing a particular product, agencies should:

- Review the guidelines and identify your records management software needs
- Review several software packages to determine which meet your requirements and match the capabilities of your staff. Software vendors can provide information and materials about their products as well as conduct on-site demonstrations. Many vendors also showcase their products at events such as the IACP Annual Technology Exposition and meetings for the Town Clerks Association, the Association of Towns, and the County Clerks Association.
- After narrowing your choices, contact other users of the products to obtain an objective review of how the software performs in a real-world situation. Do not limit your contacts only to those references provided by the vendors. No vendor would seek a reference from someone dissatisfied with the product.

RMS should support the following core records management activities:

- Identifying records series held by governments and agencies and their locations (e.g., offices, inactive storage, archives, or archival facility)
- Determining retention schedule for a record series
- Creating and maintaining inventory files
- Providing accurate reports on record series due for destruction/disposition
- Identifying vital records, confidential records, records in poor physical condition, archival records, official copies, record format types, and records to be transferred to other media
- Providing State Archives Schedules pertaining to the user government available on line
- Capturing and maintaining the fields and data elements in the form they appear on the State Archives Inventory Worksheet
- Generating standard reports such as:
  * Record series by location
  * Record series by department
  * Record series by destruction date
  * Archival series
  * Vital records
  * Confidential records
  * Format type

Reports should be easily formatted by users and able to be generated to answer ad hoc queries such as a request for a list of all records of a given department in a specific location sorted by destruction date. Reports should be made available in tabular form when required or desired.
Remember to analyze the needs of the department considering all the users. Don’t be dazzled by the bells and whistles and forget to check the nuts and bolts.

- Will the system interface with your existing computer aided dispatch (or include CAD functions)?
- Will the system report crime statistics in NIBRS format?
- Does the vendor provide 24-hour system support?
- Does the system regularly perform an automatic backup of the database?
- Will you be able to utilize any of your existing computer and network hardware?
- Will the vendor allow other software to run on the same computer?
- What are the costs of warranty and long-term support and updates?
- Is the hardware you’re buying upgradeable?
- Is training included?
- Will the vendor provide data conversion if replacing an existing system?
- If data conversion is not feasible can the systems run simultaneously?

In addition to the functionality of the software, it is necessary to consider your facility.

- Will you need additional power or network cabling?
- Are additional workstations needed?

Adapted from LEIM Guidelines for Records Management Systems, 1995 by Charles Drescher.
http://www.iacptechnology.org/LEIM/RMSGuidelines.htm
Almost all problems and failures in the implementation of a RMS can be attributed to communications problems. For example, arguments often emerge over an agency and the software service provider having different expectations of what is being delivered. Even internally in the department, differing views on what functionality is to be provided can lead to conflicts affecting successful implementation.

Paul Wormeli
Executive Director—Integrated Justice Information Systems Institute

Implementing an automated law enforcement RMS can be a trying experience. In most agencies, entrenched processes and practices will inevitably conflict with the design of software products in ways that require changes in such processes to take full advantage of the capabilities of the software. In many cases, the acquisition of an automated system can simplify processes and procedures if the department is open to reinventing the way reporting and report approval are handled. The biggest challenge in implementation is to find the right balance between doing business the way the department wants to and the way that takes most advantage of the system.

When it appears that the software is not organized to fit perfectly with the established processes, an easy resolution is to conclude that the software does not work properly. A better conclusion is often that processes should be reexamined to see if there is a way for the conflict to be resolved operationally.

At all stages of the implementation, there are ways to mitigate the risk of having an unhappy conclusion to the project. Sidestep the following ten mistakes to look good as you roll out your RMS program.

**Mistake #1** Trying to implement portions of a RMS solution...before crafting a well-defined program.

**Mistake #2** Focusing on a single business driver...instead of an overall solution.

**Mistake #3** Believing an off-the-shelf package alone can be a universal RMS solution that meets all needs.

**Mistake #4** Not understanding or distinguishing the differences between document management and records management.

**Mistake #5** Attempting to implement and deploy a total RMS program all at once...as opposed to a phased in approach, often by department.
Mistake #6  Failing to plan for the full lifecycle of the system as well as the records.

Mistake #7  Waiting for legal action against your department before considering, justifying, or implementing an effective records management program.

Mistake #8  Failing to plan for adequate initial and long-term support for the RMS program and technology.

Mistake #9  Attempting to use personnel who don’t have records management training or experience to lead the effort.

Mistake #10  Assuming that a single step or tactic can drive the strategic direction for creating an effective RMS program.

Reproduced with permission from Association for Information and Image Management E-DOC Magazine, May/June 2006. Further reproduction without express written permission is strictly prohibited.

http://www.edocmagazine.com
Estimating Costs

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

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

Cost estimating for any project is challenging, and information technology projects are no exception. As leaders of government entities, we often find ourselves in the unenviable position of having to fit initiatives into a budget that we have already been given, or request a budget increase when frankly, we may not yet have a clue what amount of money we really need for a RMS. Often, we find ourselves being driven by the availability of grant dollars, pursue a grant, and then figure out what we can buy with the money we now have.

While we must be certain to follow applicable procurement laws and guidelines, one can usually get some ballpark figures to work with that can help drive a budget request. In the same way we might visit some open houses to see the universe of possibilities and their associated cost, communication with our peers regarding recent projects and system acquisitions can often provide a good starting point. In addition, vendors are very eager to display their wares, and will sometimes be willing to provide a wide-range of the potential cost of a RMS. But, the question that will always be asked, and you should ask yourself first is: “What are my true business needs?”

A true cost estimate can only be obtained after thorough requirements analysis. One should guard against merely shopping around, looking at various packages and saying “that one looks pretty good.” It is only through a true examination of your business processes that your system requirements (which will drive cost) can be determined. This is an often arduous process, but well worth the effort. Agencies have found that an examination of business practices can reveal many areas in which processes can be improved, and discover inefficiencies that exist because “we’ve always done it like that.” The process of acquiring a RMS, and ensuring complete requirements analysis up front, can yield many additional benefits and resolution to business problems.
Initial Investment

Some items to consider regarding the initial investments necessary are included here.

- **Requirements Gathering**—Often an independent consultant can be obtained to conduct the critical requirements gathering. Consultants can be obtained on an hourly basis, or one might consider a deliverables type of contract in which a fixed price is obtained for a complete requirements analysis. A word of advice—focus on the business need of your agency for the majority of your requirements. Technology should support the business, not the other way around. Avoid utilizing a specific RMS vendor for a requirements analysis, and shy away from having a requirements gathering effort led by your technology shop. Focus on what are the business needs.

- **System Acquisition—Buy or Build**—Requirements will drive your need. A competitive bid will usually be required. Upon receiving responses to your bid, you will truly know what your costs will be. Consider asking bidders to itemize features and functionality where possible. This will provide some flexibility, and perhaps allow you to obtain basic, required features first, and continue to expand as funding allows. To see the Law Enforcement Tech Guide, published by the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS), visit [http://www.cops.usdoj.gov](http://www.cops.usdoj.gov) for a comprehensive guide to acquiring technology.

- **System Implementation**—In addition, one should consider the following which can be some high dollar items:
  - **Training**—Training costs can often be rolled into the costs of an RMS received as part of a competitive bid. Be sure to consider how to train your staff once a system is received. Some agencies will choose to utilize a ‘train the trainer’ philosophy which may, on the face, seem less expensive (in hard dollars). Don’t forget to think through the true impact of utilizing in-house personnel as your training experts. It might
  - **Hardware**—Does your RMS include mobile data computers, in-house workstations for officers, or both? What infrastructure is needed? Computer servers, printers?
  - **Networking**—What cost increases, if any, will be experienced once the system is rolled out? Will your jurisdiction use commercially provided wireless networks? What are the costs per unit, air time, etc? For internal networking, will a creation or expansion of an internal network be required?

Recurring Costs

Determining a true overall cost of ownership is often not thoroughly considered when making technology decisions. Out year costs can often come as a surprise. Here are a few things to consider:

- **Software Maintenance**—Once a RMS is established, it is important to ensure it is
maintained and updated as needed. One should consider that software maintenance on a RMS will range from 15–25 percent of the original cost of the software. Be sure to have a clear understanding as to what level of service you will receive as part of your ongoing maintenance. Does it include free upgrades if the vendor improves the product? What service does it include when problems are encountered?

- **Software Upgrades**—Attention should also be given to other software products that run on the system and impact a RMS. Updates to operation systems is a good example. Consider if the vendor or service provider ensures the continued proper functionality of your RMS given these changes.

- **Hardware Maintenance**—Hardware is often procured with a maintenance agreement as well. For larger investments, such as high end servers, maintenance contract is recommended. For lower end, more inexpensive hardware, it might make sense to have some management contingency dollars in your budget, just in case a server breaks.

- **Network Costs**—These costs are ongoing, whether they are for wireless technology or for 'hard wired' networks. Even if you or your jurisdiction administers its own internal network, costs to connect to state information providers, the National Crime Information Center (NCIC) or other connectivity will need to be maintained.

- **Ongoing Training**—Updates to the software may require some additional training for officers and other users. Will this be an additional cost, or will it be included in your software maintenance agreement. Also, will internal staff need to be trained in any technology areas?
Purchasing Guidelines
Source: Standard Functional Specifications for Law Enforcement RMS

Because of the rapidly changing nature of technology, it can be difficult to stay current on technology upgrades. Performance specifications and technology standards are the underlying “laws” that govern the development of local, national, and international services, networks and procedures. Telecommunications networks worldwide use formal telecommunications standards to physically interconnect their systems and ensure that they perform as expected. Without agreements and the standards that codify them, wide-area voice, data, and video communications would not be possible.

The LEITSC RMS Functional Specifications present functional standards for law enforcement RMS. The standards found in this document are intended to be generic in nature rather than favor one particular system or approach over another. They are at the functional level meaning that they define what is to be accomplished versus how it should be accomplished. It is intended that these standards will be updated and augmented on a regular basis.

The goals of the standards defined herein are to improve information sharing between law enforcement and other criminal justice agencies and to streamline and lower the cost of implementing and maintaining RMS.

The information in this document has been compiled from agency plans and requests for proposals, research of materials on the Internet, and documents collected from systems providers. Teams of industry and law enforcement agency personnel consolidated the information to produce this report.

Using these standards, it is anticipated that law enforcement agencies will be able to review their systems and determine if they meet the standards. Systems providers will also be able to review their products and make sure they meet the standards. Having this foundation, communications between the supplier and user community should be vastly improved.

This document was created using a modeling tool. The Standard Functional Specifications for Law Enforcement RMS developed in 2006 are invaluable in the planning and purchasing process of RMS and are available in the appendix of this desk reference as well as online.
http://www.leitsc.org
Backup Systems

By Frank Garner

The question chiefs should be asking, is what are the grades our department would receive on a “Risk Report Card” concerning our RMS?

Your agency’s organizational risk lies not only in your paper files but also in e-mail, portable computing devices, telephones, removable storage and backup tapes. With this list, administrators begin to see the full picture of organizational risk.

With the help of a professionally developed RMS assessment document plus information from fellow chiefs and vendors, you can begin to uncover your organization’s potential risk in litigation and e-discovery, should the system fail. Now is the time for due diligence.

We know that by researching RMS best practices, LEITSC Standard Functional Specifications, and case law a warning flag will be raised. This reminds us that now is the time to locate a secure, user-friendly, automated, guided self-assessment which will provide a complete diagnostic analysis of the department’s strengths and weakness in the RMS environment.

Once an analysis is completed, the department will better understand the agency’s potential for risk and it’s readiness for e-discovery and the other associated risks.

The time to start thinking about what to do if your RMS fails is now. The worst time to start planning for its failure is after it has happened. An important part of your RMSs should include an automatic backup procedure. In many cases the RMSs server automatically backs up the database every night, and that backup should then be copied to a tape backup or burned on DVD or other media. The backup files should be stored off premise.

Preparations for a catastrophic failure should include access to hardware that can support the RMS backup file medium. Access to that hardware by the people who need it is a critical element in effective planning. Power supply disruption must also be considered; uninterruptible power sources and dependable generator backup are crucial. The hardware supporting electronic RMS can be little more than a boat anchor unless electrical backup systems are in place.
When all else fails, don’t forget that RMSs started with notebook paper and a #2 pencil. Your RMS failure protocol should also include the ability to manually record events for later data entry.

Developed for IACP’s Technology Desk Reference by Chief Frank Garner, Chairman, TTAP–RMS Working Group, Kalispell Police Department—Montana
Training
By Don Post and Marcialynn Harrington

No system will be successful unless those who use it are fully trained. Agencies may be inclined to purchase less training support than is needed, on the assumption that power users will train others, but this approach has the potential for severe implementation problems that will never be fixed. Training needs and objectives should be identified early in the project and a complete training plan developed that ensures all potential users are trained to the level that they require for the system to be useful.

Some agencies have taken to including refresher training in the purchase agreement, ensuring that the software provider will return a number of months after implementation to maintain training levels. Some companies have introduced web-based training as a means to fulfill follow-up training needs. Line managers and supervisors must be fully committed to getting their staff trained, and must support the training plan and schedule to achieve this goal.

There Oughta Be a Law—Why Records Management Training Is Critical to a Department’s Success

Recently my neighbor taught his son to ride a new two-wheeler. From a distance, Sam looked like a proud expert on his “big boy bike.” Closer, you could see that Sam’s training wheels kept him upright, as did his dad’s light hold on the bicycle seat. His helmet added insurance that he could avoid serious injury if he did take a spill.

Today Sam was on his bike—wobbly, but doing fine. His training wheels were off, and his dad was not holding on. Sam had perfected balancing, now confident to go faster and farther – thanks to his training wheels.

What do Sam and his training wheels have to do with records management for police departments? Well, the principle is the same: good, solid training is the basis for confidence, efficiency, and success!

“Training Wheels and a Helmet” for Records Management

Worldwide, records management is a high-priority focus for virtually all organizations of any size, and police departments – especially those in the US and Canada – are no exception. In the U.S. federal, state, and local laws and regulations govern everything
from the definition of a record to storage, disaster recovery, retention schedules, and access.
As the paperwork of law enforcement has become more electronic-based, filing practices have eroded. What was once a file properly stored has now become a file somewhere on a network drive.

Further complicating records management is that today, “records go beyond the common paper variety,” said John Gibbons, a former New Jersey police chief now focused on records management. Gibbons continues, “non-paper records include surveillance tapes, crime-scene samples and photos, 9-1-1 recordings, videos from in-car cameras, etc.”

“In addition, police records management has always been a challenge and is becoming more so. New technologies, such as improved DNA testing, illustrate why old cases can become reactivated. When this happens, recovering old files becomes crucial to the revived investigation,” as stated by a project manager working on an award winning and groundbreaking application of computer technology to law enforcement records management.

This article assumes that the department is starting with a “bicycle”: a RMS is in place (or soon to be), all of the questions about definitions, retention schedules, access, etc., have been addressed, and a policy is firmly in place and adhered to.

So, whether as the result of the agency’s direct involvement beginning with defining requirements (the ideal), or the department’s having been an “add on” to other municipal departments, or the municipality’s governing body having determined what system should run in the police department, all that is left is the training wheels and a helmet before the department is off and rolling!

**Manage Change**

It is a truism that people resist change even when the change is guaranteed to bring a positive outcome. “We have always done it this way” or “I don’t have the time!” cannot be accepted as support for the status quo. The risks are too high and the benefits are too substantial.

The chief needs to be sure that the team understands why the move to a RMS (either an update to the current system, or as a first system) is necessary, when it must begin, who and what will be involved, and how each individual is expected to help. Understand and address their concerns directly, clarifying that the department’s migration to its new RMS is a foregone conclusion. If the department has more than 8–10 persons it may find it helpful to have a “kick-off” meeting with the users. This enables everyone to hear the same message at the same time, and ask or hear others’ questions and concerns.

**Manage Expectations**

In addition to the users’ expectations, management of those that make up the municipality’s governing body is needed as well. Everyone needs to understand what will be accomplished
by the new RMS, by whom, the expected positive outcomes, and the milestone dates. Discuss training: who will be trained, why, how, when, and how much it will cost. Offer frequent progress updates. Anticipating roadblocks and how to overcome them will help ensure meeting the aggressive, though realistic and achievable dates and deadlines for which modules will go “live”. Begin with the easiest, most-assured victories so that momentum can build off the established initial success.

**Mandate Training**

Training is much easier to postpone than to schedule and implement: there seem to be other priorities demanding attention, and training can seem like just another thing to add to an already too-long list. That is why it is necessary to mandate training. The mandate should include the clear goals and expected outcomes discussed above, and set the training date. Sooner rather than later is best.

Good, solid, effective training is absolutely critical to the success of a RMS and to the department. The proper training will ultimately help the department avoid unnecessary risk, while helping the department run most efficiently. Remember, RMS training is not an option.

**Evaluate Your Training Options**

Training options run the gamut from online training done per individual, to in-person training. Let’s look at the pros and cons in relation to the unique needs of law enforcement agencies.

**Online**—Several professional organizations offer online training in records management. As an example one offers certificate programs in both electronic records management (ERM) and enterprise content management (ECM). Each certificate program has several modules leading to a certificate. These programs are convenient and modules are available on demand, 24/7. The downside to this method of training is it is not specific to law enforcement and independent studies show lower retention rates than with live training. Statistic show that only 20-30 percent of law enforcement professionals who sign up for online training actually take the training. Locate online RMS training classes by doing a web search through your Internet browser.

**Live Workshops**—Training is at either a public or a private venue. This training will also include certificate programs in ERM and ECM which are offered in live classroom settings. Within the private consulting firm arena only one is licensed to teach the live Association for Information and Image Management certificate workshops in North America. This method provides an interactive learning environment with other trainees and the trainer. The workshops are not specific law enforcement.
Vendor Led Training—When available, training may be offered to purchasers of the vendors’ software/hardware. This approach if very focused and the vendors have knowledge of law enforcement needs. The training can be less comprehensive than users require, difficult to schedule, and outside the scope of your budget.

Consultant Training—Many consultants offer RMS training that runs the gamut from poor to excellent. But, nearly all consultants are in some way tied to a vendor or integrator, so the training ends up being less than what you need at more than you can afford.

Training Wheels and Helmet

When you begin your search for an organization to conduct your training it is strongly suggested that you look for a vendor-neutral analyst and consulting firm focusing on ERM, ECM, business process improvement, and compliance advisory services. This type of firm will help your department improve ROI (return on investment), clearly define requirements and business case, evaluate software, write requirements definitions, and deploy systems faster. Look to a consulting firm that does not sell hardware, software or system and who has a solid reputation and hopefully an office in locations near your community.

Additionally the consulting (training) firm must have substantial experience working and active connections with all levels of government, including law enforcement departments.

When a contract with either a person or corporation is established – whether to write requirements definitions, evaluate software, or conduct records management training—get exactly what you need, when you need it, where you want it, and at a rate you can afford.

Developed for IACP’s Technology Desk Reference, 2006 by Don Post, Partner—IMERGE Consulting, Inc. and Marcialynn Harrington, ERMp, ERMs, MBA, Director of Best Practices—IMERGE Consulting, Inc.

training@imergeconsult.com, (815) 398-0492
Sample Policy

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

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

Definition [Type of Government Records] Records

All documents, papers, letters, books, maps, photographs, sound or video recordings, microfilm, magnetic tape, electronic media, or other information recording media, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under the laws of the state, created or received by the [Name of Government] or any of its officers or employees pursuant to law or in the transaction of public business are hereby declared to be the records of the [Name of Government] and shall be created, maintained, and disposed of in accordance with the provisions of this [Ordinance, Order, or Resolution] or procedures authorized by it and in no other manner.

A. Additional Definitions

1. “Department head” means the officer who by ordinance, order, or administrative policy is in charge of an office of the [Name of Government] that creates or receives records. (Notes, 1)
2. “Essential record” means any record of the [Name of Government] necessary to the resumption or continuation of operations of the [Name of Government] in an
emergency or disaster, to the recreation of the legal and financial status of the [Name of Government], or to the protection and fulfillment of obligations to the people of the state.

3. “Permanent record” means any record of the [Name of Government] for which the retention period on a records control schedule is given as permanent.

4. “Records control schedule” means a document prepared by or under the authority of the records management officer listing the records maintained by the [Name of Government], their retention periods, and other records disposition information that the records management program may require.

5. “Records management” means the application of management techniques to the creation, use, maintenance, retention, preservation, and disposal of records for the purposes of reducing the costs and improving the efficiency of recordkeeping. The term includes the development of records control schedules, the management of filing and information retrieval systems, the protection of essential and permanent records, the economical and space-effective storage of inactive records, control over the creation and distribution of forms, reports, and correspondence, and the management of micrographics and electronic and other records storage systems.

6. “Records liaison officers” mean the persons designated under Section 10 of this [Ordinance, Order, or Resolution].

7. “Records management committee” means the committee established in Section 6 of this [Ordinance, Order, or Resolution].

8. “Records management officer” means the person designated in Section 5 of this [Ordinance, Order, or Resolution].

9. “Records management plan” means the plan developed under Section 7 of this [Ordinance, Order, or Resolution].

10. “Retention period” means the minimum time that must pass after the creation, recording, or receipt of a record, or the fulfillment of certain actions associated with a record, before it is eligible for destruction.

B. [Type of Government] Records Declared Public Property

All [Type of Government] records as defined in Section 1 of this ordinance are hereby declared to be the property of the [Name of Government]. No [Type of Government] official or employee has, by virtue of his or her position, any personal or property right to such records even though he or she may have developed or compiled them. The unauthorized destruction, removal from files, or use of such records is prohibited.

C. Policy

It is hereby declared to be the policy of the [Name of Government] to provide for efficient, economical, and effective controls over the creation, distribution, organization, maintenance, use, and disposition of all [Type of Government records through a comprehensive system of integrated procedures for the management of records from their creation to their ultimate disposition, consistent with the requirements of the Local
Government Records Act and accepted records management practice.

D. Notes

Version 1. Designation of Records Management Officer—The [Type of Governing Body, or Title of Chief Administrative Officer] shall designate an individual, employed by the [Type of Government], to serve as Records Management Officer for the [Name of Government]. In the event of the resignation, retirement, dismissal, or removal by action of the [Type of Governing Body, or Title of Chief Administrative Officer] of the individual so designated, the [Type of Governing Body, or Title of Chief Administrative Officer] shall promptly designate another individual to serve as Records Management Officer. (Notes, 3) The individual designated as Records Management Officer shall file his or her name with the director and librarian of the State Library within thirty days of the date of designation, as provided by state law.

Version 2. Designation of Records Management Officer—The [Name of Office], and the successive holders of said office, shall serve as Records Management Officer for the [Name of Government]. As provided by state law, each successive holder of the office shall file his or her name with the director and librarian of the State Library within thirty days of the initial designation or of taking up the office, as applicable.

E. Establishment of Committee and Duties

Establishment of Records Management Committee; Duties. (Notes, 4) A Records Management Committee consisting of the [Titles of Positions] is hereby established. The committee shall:

1. Assist the records management officer in the development of policies and procedures governing the records management program
2. Review the performance of the program on a regular basis and propose changes and improvements if needed
3. Review and approve records control schedules submitted by the records management officer
4. Give final approval to the destruction of records in accordance with approved records control schedules and
5. Actively support and promote the records management program throughout the [Name of Government]

F. Records Management Plan to be Developed; Approval of Plan; Authority of Plan

1. The records management officer and the Records Management Committee shall develop a records management plan for the [Name of Government] for submission to the [Type of Governing Body]. The plan must contain policies and procedures designed to
reduce the costs and improve the efficiency of recordkeeping, to adequately protect the essential records of the [Type of Government], and to properly preserve those records of the [Type of Government] that are of historical value. The plan must be designed to enable the Records Management Officer to carry out his or her duties prescribed by state law and this [Ordinance, Order, or Resolution] effectively.

2. Once approved by the [Type of Governing Body] the records management plan shall be binding on all offices, departments, divisions, programs, commissions, bureaus, boards, committees, or similar entities of the [Name of Government] and records shall be created, maintained, stored, microfilmed, or disposed of in accordance with the plan.

3. State law relating to the duties, other responsibilities, or recordkeeping requirements of a department head do not exempt the department head or the records in the department head’s care from the application of this [Ordinance, Order, or Resolution] and the records management plan adopted under it and may not be used by the department head as a basis for refusal to participate in the records management program of the [Name of Government].

G. Duties of Records Management Officer

In addition to other duties assigned in this [Ordinance, Order, or Resolution], the records management officer shall:

1. Administer the records management program and provide assistance to department heads in its implementation
2. Plan, formulate, and prescribe records disposition policies, systems, standards, and procedures
3. In cooperation with department heads identify essential records and establish a disaster plan for each [Type of Government] office and department to ensure maximum availability of the records in order to re-establish operations quickly and with minimum disruption and expense
4. Develop procedures to ensure the permanent preservation of the historically valuable records of the [Type of Government]
5. Establish standards for filing and storage equipment and for recordkeeping supplies;
6. Study the feasibility of and, if appropriate, establish a uniform filing system and a forms design and control system for the [Name of Government]
7. Provide records management advice and assistance to all [Type of Government] departments by preparation of a manual or manuals of procedure and policy and by on-site consultation
8. Monitor records retention schedules and administrative rules issued by the State Library and Archives Commission to determine if the records management program and the [Type of Government]’s records control schedules are in compliance with state regulations
9. Disseminate to the [Type of Governing Body] and department heads information concerning state laws and administrative rules relating to local government records
10. Instruct records liaison officers and other personnel in policies and procedures of the records management plan and their duties in the records management program

11. Direct records liaison officers or other personnel in the conduct of records inventories in preparation for the development of records control schedules required by state law and this [Ordinance, Order, or Resolution]

12. Ensure that the maintenance, preservation, microfilming, destruction, or other disposition of the [Type of Government] records is carried out in accordance with the policies and procedures of the records management program and the requirements of state law

13. Maintain records on the volume of records destroyed under approved records control schedules, the volume of records microfilmed or stored electronically, and the estimated cost and space savings as the result of such disposal or disposition

14. Report annually to the [Type of Governing Body] on the implementation of the records management plan in each department of the [Name of Government], including summaries of the statistical and fiscal data compiled under Subsection (13)

15. Bring to the attention of the [Type of Governing Body] non-compliance by department heads or other [Type of Government] personnel with the policies and procedures of the records management program or the Local Government Records Act

H. Duties and Responsibilities of Department Heads

In addition to other duties assigned in this [Ordinance, Order, or Resolution], department heads shall:

1. Cooperate with the records management officer in carrying out the policies and procedures established in the [name of government] for the efficient and economical management of records and in carrying out the requirements of this [Ordinance, Order, or Resolution]

2. Adequately document the transaction of government business and the services, programs, and duties for which the department head and his or her staff are responsible

3. Maintain the records in his or her care and carry out their preservation, microfilming, destruction, or other disposition only in accordance with the policies and procedures of the records management program of the [Name of Government] and the requirements of this [Ordinance, Order, or Resolution]

I. Designation of Records Liaison Officers

Each department head shall designate a member of his or her staff to serve as records liaison officer for the implementation of the records management program in the department. If the records management officer determines that in the best interests of the records management program more than one records liaison officer should be designated for a department, the department head shall designate the number of records liaison officers specified by the records management officer. Persons designated as records liaison officers...
officers shall be thoroughly familiar with all the records created and maintained by the department. In the event of the resignation, retirement, dismissal, or removal by action of the department head of a person designated as a records liaison officer, the department head shall promptly designate another person to fill the vacancy. A department head may serve as records liaison officer for his or her department.

J. Duties and Responsibilities of Records Liaison Officers
In addition to other duties assigned in this [Ordinance, Order, or Resolution], records liaison officers shall:
1. Conduct or supervise the conduct of inventories of the records of the department in preparation for the development of records control schedules
2. In cooperation with the records management officer coordinate and implement the policies and procedures of the records management program in their departments
3. Disseminate information to department staff concerning the records management program

K. Records Control Schedules to be Developed; Approval; Filing with State
1. The records management officer, in cooperation with department heads and records liaison officers, shall prepare records control schedules on a department by department basis listing all records created or received by the department and the retention period for each record. Records control schedules shall also contain such other information regarding the disposition of [Type of Government] records as the records management plan may require.
2. Each records control schedule shall be monitored and amended as needed by the records management officer on a regular basis to ensure that it is in compliance with records retention schedules issued by the state and that it continues to reflect the recordkeeping procedures and needs of the department and the records management program of the [Name of Government]
3. Management Committee—Version 1
   Before its adoption a records control schedule or amended schedule for a department must be approved by the department head and the members of the Records Management Committee
Management Committee—Version 2
   Before its adoption a records control schedule or amended schedule for a department must be approved by the department head, the [Title of Office of Chief Legal Officer], and the [Title of Office of Chief Financial Officer]
4. Before its adoption a records control schedule must be submitted to an accepted for filing by the director and librarian as provided by state law. If a schedule is not accepted for filing, the schedule shall be amended to make it acceptable for filing. The records
management officer shall submit the records control schedules to the director and librarian.

**L. Implementation of Records Control Schedules; Destruction of Records Under**

1. A records control schedule for a department that has been approved and adopted under Section 12 shall be implemented by department heads and records liaison officers according to the policies and procedures of the records management plan.
2. A record whose retention period has expired on a records control schedule shall be destroyed unless an open records request is pending on the record, the subject matter of the record is pertinent to a pending law suit, or the department head requests in writing to the Records Management Committee that the record be retained for an additional period.
3. Prior to the destruction of a record under an approved records control schedule, authorization for the destruction must be obtained by the records management officer from the Records Management Committee.

**M. Destruction of Unscheduled Records**

A record that has not yet been listed on an approved records control schedule may be destroyed if its destruction has been approved in the same manner as a record destroyed under an approved schedule and the RMS officer has submitted to and received back from the director and librarian an approved destruction authorization request.

**N. Records Center**

A records center, developed pursuant to the plan required by Section 7, shall be under the direct control and supervision of the records management officer. Policies and procedures regulating the operations and use of the records center shall be contained in the records management plan developed under Section 7.

**O. Micrographics**

Unless a micrographics program in a department is specifically exempted by order of the [Type of Governing Body], all microfilming of records will be centralized and under the direct supervision of the records management officer. The records management plan will establish policies and procedures for the microfilming of [Type of Government] records, including policies to ensure that all microfilming is done in accordance with standards and procedures for the microfilming of local government records established in rules of the State Library and Archives Commission. The plan will also establish criteria for determining the eligibility of records for microfilming, and protocols for ensuring that a microfilming program that is exempted from the centralized operations is, nevertheless, subject to periodic review by the records management officer as to cost-effectiveness, administrative efficiency, and compliance with commission rules.
Notes

1. This provision is modeled after the definition of “custodian” in the Local Government Records Act (201.003(2)). That definition reads: “Custodian means the appointed or elected public officer who by the state constitution, state law, ordinance, or administrative policy is in charge of an office that creates or receives local government records.” The authority under which a person serves as a custodian of the records of a local government office varies from government to government. The definition in the ordinance or order should be modified to suit the circumstances of each government.

2. It is important that either one or the other of Section 5 (or a similar provision in those larger governments that have full-time records managers) appear in the ordinance or order, despite the fact that the records management officer may already have been designated in a previous action of the governing body.

Either one or the other of these sections can be modified appropriately if the local government, through a contract or agreement under the Interlocal Cooperation Act (Article 4413(32c)), will have records management services provided by a records management officer employed by another local government or by an administrative agency created under the contract or agreement.

State law, however, charges governing bodies with duties and responsibilities designed to promote the effective and efficient management of records and the preservation of historical resources. The records management officer will be the principal agent of the governing body for implementing the ordinance or order and because the records management program will affect every department of the local government, it is a matter of managerial efficiency that there be as few intermediary personnel between the records management officer and the governing body as possible.

If a part-time records management officer is designated, he or she should be someone whose other duties are commensurate with the government-wide responsibilities and authority for the local government’s records program as provided by state law and this ordinance or order.

In larger governments, a records management program headed by a full-time, professional records manager should never be accorded anything less than the sub-department status in the organizational chart of the government.

3. Although state law directs the governing body to designate a records management officer, nothing in the law prevents the governing body from delegating this authority to the chief administrative officer, who may customarily appoint other department and program heads. The name of the individual designated must still be entered in the minutes of the governing body although he or she may have been designated by the chief administrative officer.

Local governments with full-time, professional records managers sometimes dispense with the establishment of a formal records management committee under the assumptions that the records manager is a professional who is well versed in the principles and strategies of effective records management and that he or she will consult on a regular basis with the appropriate officials in the development of a formal program. A decision not to establish a records management committee either in small governments or in governments with records management departments does not affect the need for approval of records control schedules provided for in Section 12.

The duty described under Subsection (d) is optional for this committee, but should not be optional for the program. Destruction of records under an approved schedule should not be fully automatic. State law forbids the destruction of records on which either an open records request or a law suit is pending, although the
retention periods for the records may have expired. There may also occasionally be other factors that warrant keeping a record beyond its retention period. Provision should be made, as it is in this model in Section 13, for the final approval for the destruction of records under an approved schedule by either the records management committee or other officers, if a records management committee is not formed.

4. If a records management committee is not established, this section should be amended to direct the records management officer alone to prepare a plan for adoption or to designate certain officers of the government to assist in the development of the plan. The difference between the formal committee of Section 6 and a group of officers designated to assist in this section is that the latter is ad hoc and temporary and will play no continuing role in the records management program unless specified to do so in other sections of the ordinance or order.

This Subsection may be in the records management plan and not the ordinance or order. It is included here because of its crucial importance in successful records management programs. One of the fundamental tenets of records management is that a record be destroyed when its value has ceased for the organization that maintains it. The duration of the record’s value has already been determined by the setting of the retention period on the records control schedule. Barring, therefore, pending open records requests or lawsuits or the occasional special circumstance, a local government’s records management program should provide for the mandatory destruction of records whose retention periods have expired. Discretionary programs in which department heads may dispose of records under schedule never result in the benefits in cost and space savings and administrative efficiency a well-designed program is designed to deliver. In practice, the submission of requests from department heads for an extension of a retention period may result in the amendment of the retention period on the records control schedule.

A sample policy courtesy of the IACP Technology Technical Assistance Program—October 2006
Sample Press Release

Source: Government Technology

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

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

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

NEWS FOR IMMEDIATE RELEASE | January 1, 2010

Anytown, Police Department Updates Records Management System

January 1, 2010

New system reduces paper use, gives detectives timely access to reports and provides information on who is accessing the information

The Anytown Police Department (APD) works to serve and protect its city of (population size) citizens. As the capital of state, the APD’s (number) sworn officers are also responsible for providing safety to the city’s one million annual visitors who come to see the historic sites the area has to offer.
Given this responsibility, APD is constantly looking for ways to make its officers and detectives more efficient. One area where a need for improvement was identified was in the department’s storage and retrieval of police incident reports and APD turned to an electronic records management system.

Prior to the new system, APD records staff retrieved hard-copy police reports, accident reports, drug and alcohol reports and supplemental reports from various departments throughout the jurisdiction. Totally manual access to these reports required personnel to locate files, make copies and archive additional reports as materials were produced. Paper copies were then disseminated to various APD personnel and such others as the courts, state’s attorney general, and public defenders.

“The manual process required significant staff resources and was frustrating for detectives who needed timely access to reports,” according to Deputy Chief Paul Smith. “Prior to the new system, detectives used to spend an average of ½ hour retrieving a report and the process involved a trip to the records department. Now they can access the same information in just a few seconds, right at their desks.”

With the new system, paper reports with the minimum required information are scanned and stored in a searchable database. Officers and others requiring information from the system can then find the desired information by searching filed reports by over 20 different criteria including the date of the incident, names of involved parties, the names of witnesses or the names of suspects. The system also includes a database of street addresses in Springfield that allows officers to find out information on crimes committed at a single location.

In addition to the saving time and eliminating the backlog and expense of microfilm, APD has also realized a number of other unforeseen benefits as a result of the new RMS. “Security was a significant concern with an electronic system but we have found that our records are actually more secure now since we know exactly who looked at, printed, or e-mailed every record in the database,” according to Smith. “We have also gained round the clock access to records so the 2nd, 3rd, and weekend shifts no longer have to wait for the records department to be open during normal business hours before they can retrieve a report.”

The system has also proven to be very simple to use and has helped investigators uncover potentially related incidents because officers are able to easily run searches on individuals, addresses, dates, and Uniform Crime Report (UCR). The system is also easy to administer since it is completely Web-based and no software needs to be installed on any APD workstations.

Reprinted with permission from Government Technology magazine. Further reproduction without express written permission is strictly prohibited.

http://www.govtech.net
Legal Issues
Source: Institute for Intergovernmental Research

Legislative restrictions related to RMSs are in place in Federal and state statutes. Federal laws prohibit dissemination of computerized criminal history information where disposition is not also provided, and limit their use to criminal justice purposes. While this legislation normally addresses the conventional rap sheet, aggregate data from a RMS is also covered.

State legislation varies and should be considered in defining system operation and local practices. Most states have independent statutes governing sealing and purging, and such legislation will impact the data retention policies that should be implemented with an RMS. States typically empower the courts to determine when and if individual arrest records are sealed and procedures in the RMS should conform to state law on these matters. Police agencies should also be aware of state laws and regulations affected reporting dispositions and ensure that the necessary steps are being taken to submit information that can be accommodated in the state’s automated criminal history repository.

http://www.firstgov.gov/Topics/Reference_Shelf/Laws.shtml
http://www.arma.org/legal/index.cfm


Compliance
28 CFR Part 23 is a guideline for law enforcement agencies. It contains implementing standards for operating federally funded multijurisdictional criminal intelligence systems. It applies to systems operating through federal funding under the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

It provides guidelines for:
- Submission/Entry of Criminal Intelligence Information
- Security
- Inquiry
- Dissemination
- Review and Purge
It does not provide specific, detailed information on how the standards should be implemented by the operating agency.

Each agency develops its own operating policies and procedures, including who can have access to the information, submission format for entry of information, types of criminal activity to be maintained in the system, validation and purge procedures, security, audit and inspection, forms, participation agreements, and so forth.

These policies and procedures vary from agency to agency and, in some instances, may be more restrictive than 28 CFR Part 23 would require.

Agencies maintain reports, files, and databases (not operated with federal funding) which contain investigative or management information, some of which would meet 28 CFR Part 23 requirements and some of which would not. Information which meets 28 CFR Part 23 requirements may be gleaned from this documentation and entered into the intelligence database.

Single agency databases where no information is disseminated or shared outside the agency do not have to comply with 28 CFR Part 23 requirements. Agencies may collect information through their normal agency investigative processes and maintain that information in their agency files. As long as that information is only used within the agency, 28 CFR Part 23 does not apply. However, if the information is elevated to a multijurisdictional intelligence database where it will be shared with multiple agencies, then it must meet 28 CFR Part 23 requirements.

**Interpretations**

Because the 28 CFR Part 23 requirements are not precisely defined, the Office of General Counsel, Office of Justice Programs, U.S. Department of Justice, has rendered interpretations that govern the operation of these criminal intelligence systems. These interpretations are incorporated throughout this brochure.

**Entering Names of Individuals and Organizations in the Database**

The officer submitting the information must have enough information from sources, observations, or other investigative efforts to believe the named subject (individual, organization, group, or business) is involved in criminal activity.

The subject does not have to be the target of an investigation. The subject does not have to have been arrested. Officials of the Office of Justice Programs and the Bureau of Justice Assistance have interpreted this provision to apply to all names for which a record or file is created in the database:
• Individuals
• Associates
• Relatives
• Employers
• Telephone subscribers
• Organizations, groups, or gangs, including extremist groups
• Businesses
• Corporations, etc.

Names of organizations, groups, and businesses, which are part of a criminal enterprise or are a front for criminal activity can be entered.

The suspected criminal activity of the subject (individual, organization, group, or business) should be listed in the database.

Backup documentation supporting the determination of the suspected criminal activity of the subject must be kept in the submitting agency files.

If an organization, group, or business is documented as a criminal enterprise or front, the members are considered to be reasonably suspected of involvement in the specified criminal activity and can be entered in the database.

**Non-Criminal Identifying Information**

Under the following circumstances, names of individuals, organizations, groups, or businesses that are not suspected of criminal involvement but that provide descriptive, identifying information regarding the criminal suspect may be entered as “noncriminal identifying information”:

• The information must be labeled or contain a disclaimer that it is noncriminal identifying information
• The criminal suspect identified by this information must meet all requirements of 28 CFR Part 23
• The identifying information cannot be used independently to meet the reasonable suspicion requirement needed to create a record or file in the database

**What Not to Enter**

Do not automatically enter names of all individual members of organizations, groups, or businesses without a determination that the organization, group, or business is a criminal enterprise or front.

Do not create and maintain a record or file on an individual unless the individual is suspected of criminal activity.
Do not enter names of individuals, organizations, groups, etc., not suspected of criminal activity unless clearly labeled as “non-criminal identifying information.”

No information about political, religious or social views, associations, or activities can be entered unless the information relates to criminal activity and the subject is suspected of criminal activity.

Information obtained in violation of local, state, or federal laws cannot be entered.

**Database Operation**

**Set Up**—When setting up the database provide for the following information to be listed for each criminal suspect (individual or organization) entered in the database.

- Source Reliability (Reliable; Usually Reliable; Unreliable; Unknown)
- Content Validity (Confirmed; Probable; Doubtful; Cannot be Judged)
  - Entering the combination of “Unknown Source” and “Content Cannot be Judged” would not meet 28 CFR Part 23 requirements and should be blocked from entry
- Submitting Agency Name
- Submitting Officer Name

Provide for all names (individuals and organizations) entered in the database as criminal suspects to be linked to a criminal activity. National Crime Information Center (NCIC) offenses are recommended as a standard, but may not be all inclusive for agency needs. The Office of General Counsel, Office of Justice Programs, has approved use of the following criminal activity descriptions in addition to the NCIC offenses:

- Terrorism
- Narcotics
- Criminal Gang
- Street Gang
- Prison Gang
- Security Threat Group
- RICO
- Labor Racketeering
- Organized Crime

Provide for sufficient data to be entered to identify the subject (date of birth, race, sex, etc.)

Provide the capability to label or add appropriate disclaimers for each name (individual, organization, group, or business) entered in the database as strictly identifying information, carrying no criminal connotation. Non-criminal identifying information may only be entered as an addition to a criminal suspect’s record existing in the database. It is permissible for
these names to be searchable. Upon retrieval, it must be clear to the user that the information is non-criminal identifying information relevant to the criminal suspect, activity, or enterprise.

Provide for entry of the submittal date or the purge date (or both) so that a determination can be made of how long the information has been in the system and when it is due for purge.

Provide for capturing an audit trail of dissemination of information from the database. A record must be kept of: who received the information; the date disseminated; and the reason for release of the information.

**Purging Data**—Provide for purging data in the database prior to the expiration of the retention period (no longer than five years).

A policy may be adopted to purge submittals at the end of the retention period without any further review and validation, or a process may be adopted to validate and update the retention period of submittals which continue to comply with 28 CFR Part 23.

The purge date of a record may be updated (extended) based on validation by the submitting agency/officer that the subject continues to be suspected of criminal activity.

Agencies/officers in different jurisdictions may have information on and interest in the same subject(s). Each of the agencies may submit its own entry of the subject to the database. This would result in creating duplicate subject records that show different purge dates. Maintaining duplicate records would prevent the purge of subject information which may be of interest to agencies in more than one jurisdiction.

**Administrative and Security Issues**—Provide for security of the system, including user identification, passwords, audit trails, or other security hardware and software, to prevent unauthorized access to the information.

Provide for a written agreement to be signed by each participating agency to certify willingness to comply with 28 CFR Part 23 standards and system requirements.

Provide a process for audit and inspection of backup documentation supporting participating agency submittals to the database. This process can be conducted by mail utilizing a random sample of submittals and requesting the participating agency head certify compliance of the entry.

Obtain approval from the Office of General Counsel, Office of Justice Programs, for remote terminal access by participants to the system.
The agency operating the system must make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation, and no violation of the Electronic Communications Privacy Act (Title III) or any applicable state statute related to wiretapping and surveillance.

Want to Read the Guideline?—The complete text for the 28 CFR Part 23 guideline and text of a policy clarification is on the World Wide Web at: http://www.iir.com

Institute for Intergovernmental Research
e-mail: 28cfr23info@iir.com; (850) 385-0600, ext. 266

You may also contact staff at one of the Regional Information Sharing Systems (RISS) centers for answers to your questions about compliance. The RISS Program is funded by the U.S. Department of Justice, Bureau of Justice Assistance, and is designed to enhance the ability of local, state, and federal law enforcement member agencies to identify, target, and remove criminal conspirators. To accomplish this mission, each regional center maintains a centralized database on thousands of criminals. These databases comply with the 28 CFR Part 23 guideline.
Additional Resources

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

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

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

Chief Paul Schultz
Lafayette Police Department—Colorado
Federal Regulation 28 CFR Part 23
28 Code of Federal Regulations A guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems.

Global Justice XML Data Model (Global JXDM)
Is intended to be a data reference model for the exchange of information within the justice and public safety communities. The Global JXDM is sponsored by the U.S. Department of Justice (DoJ) Office of Justice Programs (OJP), with development supported by the Global Justice Information Sharing Initiative’s (Global) XML Structure Task Force (GXSTF).

IACP Technology Clearinghouse
Serves as a one-stop shop for technology related information that addresses all aspects of public safety from line personnel to senior executives.

Integrated Justice Information Systems Institute (IJIS)
The mission of the IJIS Institute is to apply the expertise of industry to assist the justice and public safety community in the innovative and effective use of technologies to better share information in a way that benefits industry, the public sector, and society as a whole.

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

Law Enforcement Information Technology Standards Council (LEITSC)
LEITSC is comprised of four of the nation’s leading law enforcement organizations, specifically, the International Association of Chiefs of Police (IACP), National Organization of Black Law Enforcement Executives (NOBLE), National Sheriffs’ Association (NSA), and Police Executive Research Forum (PERF). The mission of LEITSC is to foster the growth of strategic planning and implementation of integrated justice systems.
National Information Exchange Model (NEIM)
A partnership of the U.S. Department of Justice and the U.S. Department of Homeland Security, is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations.

http://www.niem.gov/files/NIEM_Executive_Briefing.pdf

National Incident-Based Reporting Systems (NIBRS)
Is an incident-based reporting system for crimes known to the police. For each crime incident coming to the attention of law enforcement, a variety of data are collected about the incident. These data include the nature and types of specific offenses in the incident, characteristics of the victim(s) and offender(s), types and value of property stolen and recovered, and characteristics of persons arrested in connection with a crime incident.

http://www.icpsr.umich.edu/NACJD/NIBRS/

Police Executive Research Forum (PERF)
A national membership organization of progressive police executives from the largest city, county and state law enforcement agencies. PERF is dedicated to improving policing and advancing professionalism through research and involvement in public policy debate.

http://www.policeforum.org

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

http://www.search.org
Glossary

A

ACH (Arrest Charge Number)—This number provides ranking order of the charges for which the person was arrested.

ADN—An arrest-related code, arrest disposition, indicating how the arrestee was handled or referred following an arrest.

Archive—A collection of computer files that have been packaged together for backup, to transport to some other location, for saving away from the computer so that more hard disk storage can be made available, or for some other purpose.

Arresting Agency—The NCIC or ORI number of the agency that performed the arrest functions.

B

Booking Agency—The NCIC or ORI number of the agency where the arrested individual was booked.

C

Case Number—The numeric identifier assigned to a particular incident. May be synonymous with the incident number.

CCD—The Charge Codes indicate the origin for the type of charge that was assigned.

Chain of Custody—A series of log entries that indicate control, contact and movement of a piece of property while in the custody of the agency.

Compliance—Either a state of being in accordance with established guidelines, specifications, or legislation or the process of becoming so.
Computer—A device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed.

Controlling Agency—The NCIC or ORI number of the agency that is in control of the original incident or case information.

Criminal Activity—The level of the infraction – felony, gross misdemeanor, misdemeanor, petty misdemeanor, warrant, other.

G

GEO Code—The geographical designator or map number reflecting a location.

GOC (General Offense Character)—Indicates the code of the offense at the time of the arrest.

I

Incident—An event, call for service or request for response where a law enforcement department responds and generates a report of the actions.

Incident Number—The number assigned by the agency to each Incident Report to identify it uniquely. This number can be up to 12 characters and can be the actual case number (OCA) or another number.

ISN (Incident Sequence Number)—A sequential number assigned to multiple offenses occurring for one case.

J

JDN—An arrest-related code, juvenile disposition, indicating how a juvenile was processed following a booking event.

Juvenile—An individual under 18 years of age.
L

Location Grid Number—The locally defined identifier reflecting a specific area of the community or a specific location.

M

Master Indices—Serves as an internal or external portal for information sharing.

MNI (Master Name Index)—Links an individual master name record to every event in which the individual was involved or associated.

Module—An independent portion of an RMS software application that provides specific functionality.

Modus Operandi - The specific “method of operating” characteristics pertaining to the method a particular criminal uses to commit a particular crime.

MOI (Master Organization Index)—Provides an agency with a detailed, searchable store of information about organizations.

MLI (Master Location Index)—Provides a means to aggregate information throughout RMS bases on a specific address, a range of addresses, an area, and/or locations based on X/Y/Z coordinates.

MPI (Master Property Index)—The central access point that links all property records.

MVI (Master Vehicle Index)—This index provides an agency with a detailed, searchable store of information about vehicles.

N

NCIC—The National Crime Information Center is responsible for setting standards and maintaining the national database repositories used to collect crime data.

NCIC Number—The agency identifier number assigned at the federal level by the National Crime Information Center (NCIC) giving a unique number to each agency. This number, together with the Case Number, allow a multi-agency Records Management System to assign the same Case Number to different cases.
NIBRS—National Incident-Based Reporting System

O

ORI—Number identifying number assigned to the law enforcement agency by the National Crime Information Center (NCIC).

P

PRC—The Property Recovery Code indicates where an item was recovered (within or outside of a jurisdiction).

PSN—The Person Sequence Number is a unique sequential number used to define each individual arrested in a specific case. The values cannot be reused for an incident.

PTC—The Property Type Code defines property items into like classifications.

R

Reboot—To restart a computer and reload the operating system. The Ctrl-Alt-Delete keystroke combination was developed as an easy way to reboot a computer that would nevertheless be an unlikely accidental keystroke combination.

Record—A collection of data items arranged for processing by a program.

Records Management—The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the process for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

RVL—The Recovered Value is the monetary value of the property when it was recovered.

S

Standard Outputs—Query and retrieval by name, vehicle, location, organization, and/or property to produce a comprehensive response displaying all related records in the system.
STU—The Statute/Ordinance Number is the code assigned to the specific offense as listed in the agency’s legal ordinance book or a state statute.

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

SVL—Stolen Value is the monetary value of a property item that was reported as stolen.

TSN—The Type Sequence Number is a sequential number used to identify property.

UCR (Uniform Crime Reporting Program)—The three-digit code used for identifying offenses. The codes are unique to NIBRS but were derived from the four-digit NCIC Uniform Offense Classification (UOC) Codes.