HANDBOOK FOR ACQUIRING A RECORDS MANAGEMENT SYSTEM (RMS) THAT IS COMPATIBLE WITH THE NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS)

May 2002

TABLE OF CONTENTS

INTRODUCTION

This handbook has been developed under the sponsorship of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the Bureau of Justice Statistics (BJS). It provides comprehensive, step-by-step guidance to local law enforcement agencies that are, or are considering, implementing an automated incident-based Records Management System (RMS) that is compatible and compliant with the National Incident-Based Reporting System (NIBRS).

This handbook provides instructions on how to prepare for and conduct a system acquisition and prepare the agency for conversion to the new system and to NIBRS. It includes lessons learned from other agencies and from vendors and presents relevant templates and examples. The goal of this publication is to take the guesswork out of purchasing a NIBRS-compliant RMS.

The Need for Records Management Systems. Law enforcement agencies must maintain accurate, easily accessible records of the information that is relevant to law enforcement and public safety in their community. Examples of information maintained include names and addresses, incident and arrest data, case information, property and evidence data, information on permits, licenses and registrations, and crime statistics. Computer-based RMSs have been designed to help law enforcement personnel in these record-keeping tasks.

There are many RMS vendors that offer a variety of commercial off-the-shelf (COTS) capabilities and features. Not every local agency will use one of these COTS products. Some very small local agencies have difficulty getting budget approval for the purchase of any automated system; some larger agencies have custom-designed their own RMS to meet their unique needs. A law enforcement agency modernizing its record-keeping system must follow a careful path in choosing a commercial system that best meets its individual needs. A first step, of course, is understanding and documenting those needs.

Incident-Based Reporting and RMS. In the majority of cases, law enforcement agencies report crime statistics to state agencies and the FBI, and the RMS must support this procedure. Over 70 years ago, standards were established for the Uniform Crime Reporting (UCR) Program so agencies could report their crime and arrest information in the same format and at the same level of detail and accuracy. Under the traditional UCR system agencies report monthly aggregate counts for eight Index crimes. This is now referred to as *Summary UCR*.

In 1989, the FBI instituted a new crime-reporting system called the National Incident-Based Reporting System to provide a more detailed and comprehensive view of crime in the United States. Since many local law enforcement agencies continue using Summary UCR format, the FBI's CJIS Division wants to aid these

agencies in converting to NIBRS. Many of these agencies will have to make changes in how crime information is collected, processed, reported, and how quality is controlled. And many may have to move to a new or upgraded RMS.

NIBRS provides local agencies an enhanced picture of crime in their jurisdictions. Law enforcement agencies benefit in several ways from the detailed, accurate, and more meaningful data that NIBRS produces. NIBRS data help in the effective allocation of resources in the war against crime. Armed with comprehensive crime data, local agencies can better make their case to acquire the resources needed to fight crime. Local agencies that are currently certified to report NIBRS in their state affirm that:

- NIBRS improves crime classification processes.
- NIBRS provides substantial investigative benefits, including better crime analysis and crime mapping.
- NIBRS produces better information and a more readable report.
- NIBRS offers automation opportunities for improved business flow within the agency and to other entities requiring complete incident data (e.g., courts).
- NIBRS improves community policing.
- NIBRS promotes thorough crime scene data collection.

NIBRS agencies also report that officers display a higher level of concern for victims during the questioning necessary for completing an incident-based report.

The participation of local law enforcement agencies in NIBRS is important for producing a highly accurate representation of crime. Crime data accuracy and completeness provide important snapshots of crime at all levels of law enforcement: local, regional, state, and national. The crucial starting point of this crime reporting process is at the local level.

This handbook provides law enforcement agencies a detailed map for converting to a NIBRS-compliant RMS. It is a companion document to a cost model that helps law enforcement agencies estimate the costs of implementing and operating such a system. A prototype cost model was developed for the FBI and BJS as documented in *Costs of Implementing and Operating a NIBRS Capable Records Management System*, (Mitretek Systems, 14 June 1999). This Excel-based cost model has been updated through surveys of local and state agencies and vendors of NIBRS-compliant RMSs. The cost model is flexible, accommodating agencies of various sizes and levels of experience with incident-based reporting.

The sections of this report correspond to the major activities involved in moving to a NIBRS-compliant RMS as described in the "Map to Handbook," on the next page. Each section includes a summary of lessons learned, as provided by law enforcement agencies that have already implemented, or are implementing, a

NIBRS-compliant RMS, and by RMS vendors with experience in installing RMSs in agencies of various sizes.

The report is comprehensive, in order to address the broad range of functional needs of large law enforcement agencies. However, in many of the sections, text that provides guidance specifically designed for small agencies is emphasized in a "For a small agency" text box.

Map to Handbook

Section	Title	Description
1	Make the NIBRS-RMS decision	Describes the steps an agency should follow in deciding to use a NIBRS-compliant RMS and outlines information necessary to make this decision.
2	Define the RMS	Describes the process for defining RMS capabilities and requirements.
3	Develop Costs and Funding Sources	Addresses how to estimate costs and describes other cost and funding considerations.
4	Select RMS Vendor	Addresses the specific procedure agencies should follow if they decide to use RMS vendors.
5	Plan and Manage Implementation	Describes activities necessary for managing RMS and NIBRS implementation.
6	Install RMS	Describes how to prepare for and install the new computer-based RMS.
7	Agency Preparation	Provides a guide to prepare agencies to operate the new NIBRS-compliant RMS. Note: activities described in section 7 should be performed simultaneously with those described in sections 1 through 6.

1 MAKE THE NIBRS RMS DECISION

Each agency interested in acquiring a NIBRS-compliant RMS must initially assess the impact of converting from Summary UCR to NIBRS reporting. Not every agency is prepared for making this conversion and maintaining the new system once it is implemented. This section addresses the major factors that must be considered in making the decision to proceed. The subsections below address these factors:

- Justification for system change.
- Project goals and scope.
- Estimated cost.
- Operation and maintenance costs and options.
- Funding options.
- Organizational commitment.

The decision process and the information supporting the final decision should be outlined in a *strategic plan*. The strategic plan provides a high-level vision of the goals, scope, and projected benefits and costs of the new RMS project. This plan helps to explain the project to other organizations, gain the support of the community, and justify the funding needed for implementation.

1.1 Justification for System Change

Acquisition of a modern NIBRS-compliant RMS can be justified to the community and potential funding sources by documenting the serious record management problems currently faced by the agency, showing how a NIBRS-compliant RMS addresses those problems, and emphasizing additional benefits of NIBRS. (See Table 1.1.)

Depending on the scope of an agency's RMS project, implementing the RMS in phases may be advisable, although it is certainly not required. Problems can be prioritized so that the most important ones are addressed first, with lesser problems addressed as funding and scheduling permit. Table 1.1 illustrates a hypothetical agency whose implementation is accomplished in phases and whose high priority problems include difficulty in cross-referencing names and addresses and excessive time needed to prepare incident reports.

An agency can develop approaches for acquiring, implementing, and operating a NIBRS-compliant RMS, which alleviates these or other problems, by conversing with other agencies and RMS vendors. This can help an agency define the goals and scope of the RMS project, determine how the current records management and reporting problems will be addressed by a new RMS, and quantify the amount of time and effort needed to complete the project.

Table 1.1 Examples of Problems Addressed by a Modern RMS, Using a Phased Implementation Approach

Problem	Solution
Phase I:	
Inability to easily cross-reference names and addresses between files.	Acquire an RMS with central name and address file.
Time to prepare incident reports is too long with too many errors.	Acquire Automated Field Reporting module with entry-level editing, etc. for use on mobile data computers.
State and FBI crime reporting is time-consuming because of errors and cumbersome procedures.	Acquire an RMS capable of accurate NIBRS reporting.
Crime analysis is incomplete and inaccurate because of incomplete data.	Collect incident and arrest data that encompass NIBRS reporting requirements.
Phase II:	
Case management files are manual and unwieldy.	Acquire an RMS module with case management support capability.
Real time information (regarding calls for service) is not readily available for beat officers.	Provide report to each patrol shift showing all calls for service on their beat.
Phase III:	
Evidence management is time consuming and prone to errors.	Acquire property and evidence management module.

1.2 Project Goals and Scope

Once the agency knows what is achievable, the RMS project's goals and scope can be documented. Each goal should be related to an overall agency goal. Goals should be stated at a high level but should address specific problems or challenges. For example, the agency's goal might be:

Improve community policing by modernizing our records systems to:

- *Allow officers to more readily identify and locate wanted individuals.*
- *Provide officers with more time on the beat by reducing the time needed for report preparation.*
- *Assist officers in case investigations through the use of modern information storage and retrieval technology.*
- *Provide officers with information about all recent incidents occurring on their beat.*
- *Improve the safe management of evidence and other agency property*
- *Improve crime reporting and be consistent with state and federal requirements.*

As Table 1.1 exemplifies, the problems the agency currently faces and the shortcomings of current system help define the scope of the project. In addition to current problems and system limitations, the project's scope is shaped by any system interfaces that are required. For example, if the agency already has a viable case management system, then the project's scope would not include a new case management capability. However, the new RMS may need to interface with the legacy case management system and this requirement would need to be in the project's scope.

Other boundaries of the system can be defined by how the new RMS is to relate to other systems or agencies. For example, it must be determined who will enter warrant information. If the courts are to provide this information electronically to the RMS, then the electronic interface with the court system must be in the project's scope. Table 1.2 summarizes some of the broad range of functions that may be supported by a modern RMS.

Table 1.2 Potential RMS Functions

- Master name and address file
- Automated Field Reporting System supporting Mobile Data Computers
- Reports entry and processing
- Booking
- Crime analysis
- State and national NIBRS reporting
- Management reporting
- Case management
- Property and evidence management
- Pawn tracking
- Intelligence support
- Citation and traffic accident tracking and reporting
- Access to state message switch for NCIC, NLETS, III, and state crime records
- Access to computer-aided dispatch (CAD) records
- Access to geo-files of crime information
- Access to fingerprint identification system records
- Access to or copies of vehicle registration files, drivers license files, court files, Corrections files, probation files, etc.
- Registration and licenses management (gun registration, bike registration, hacker Licenses, etc.)
- Personnel administration and records maintenance
- Staffing and scheduling administration
- Training administration
- Property inventory administration

1.3 Estimated Cost

It is essential to estimate the cost of the new NIBRS-compliant RMS as part of the strategic plan. Fortunately, an agency can use an existing cost model to make this preliminary cost estimate.

In 1999, Mitretek Systems quantified the costs that law enforcement agencies could expect to incur when implementing a NIBRS-compliant RMS. From this, Mitretek developed a personal computer-based cost model with a simple graphical user interface (GUI) for the FBI and BJS staff so that they can estimate the cost of an agency's conversion to a NIBRS-compliant RMS.

This cost model, which is based on Microsoft Excel™, has been updated. Instructions have been developed so local law enforcement agencies can also use it. In general, the information needed to use the cost model includes the agency's current state of technology (no RMS, non-incident-based RMS, or incident-based RMS), monthly incident rate, number of sworn officers, and software acquisition preference (COTS or customized). (Section 3 of this report further describes the cost model and its use in more detail.)

The model generates a cost estimate for:

- Software procurement.
- Hardware procurement.
- End user and system administrator training.
- Installation services.
- Data conversion services.
- Annual operation and maintenance.

To use the model for a multi-year project, agencies may need to allocate project costs by year. For example, expenditures for the hardware and software may occur in one fiscal year, while the training, installation and data conversion costs may be incurred the following fiscal year. The operation and maintenance (O&M) costs will accrue for all years following installation.

For a small agency, the major costs are for the RMS and the desktop computer that it uses. Vendors can provide estimates for annual maintenance costs.

If an agency adopts a phased implementation approach, the costs should be identified for each phase. For example, if property management capabilities are added in a later phase then costs of the property management software module and property file conversion should be attributed to that phase.

1.4 Operational and Maintenance Costs and Options

Part of determining the feasibility of RMS and NIBRS implementation is addressing how the system will be operated and maintained, and who will be fiscally and operationally responsible. For annual fees, the hardware vendor can maintain the hardware and the commercial RMS vendor the software. But there are other O&M costs, including:

- Data entry to maintain the RMS files.
- NIBRS report preparation and quality control.
- O&M of supporting systems such as communications networks, database management systems, power, air conditioning, etc.
- Supplies.
- System changes over time to meet the changing needs of the agency. (RMS vendors can quote prices to modify their software, but this practice has serious implications.)
- System administration and performance management.
- Project oversight and quality control (to make sure implementation is being done well and on time).
- Audits of update transaction logs and reviews of security and intrusion logs.

There are three operating options:

1. **Agency assumes responsibility.** In this case, the agency must hire, train, and retain a staff with skills and knowledge needed for system O&M.

2. **Off-site Outsourcing.** The agency contracts with another government agency or commercial firm to assume responsibility for O&M.

3. **On-site Integration Contractor.** The agency contracts with a commercial firm to operate the system on the agency's premises, supply the needed personnel, and take care of day-to-day operations.

For a small agency, it may be worth considering having a nearby, larger law enforcement agency operate the RMS. A downside of this is that a smaller agency's requirements may be secondary to the larger agencies, forcing the smaller agency to accept the system as it is. Another option is to join forces with other nearby law enforcement agencies and jointly develop a shared processing facility. A downside of this shared effort is that an agency must be able to work very closely with these other agencies through a sustained, intense effort. Unless a well-defined decision-making process exists, or unless one agency acts as the lead agency, the joint effort will tend to come apart due to the strains of the effort.

Outsourcing or integration contracting may be attractive alternatives if an agency is unlikely to be able to staff RMS operations; however, there are a few cautions. First, the agency must be prepared to turn over custodianship of its information to a trusted entity. Second, the agency must retain in-house knowledge of its system and provide management oversight of the contractor's performance to ensure that its needs are met. Third, projected costs may be more than the agency expects.

1.5 Funding Options

Several options may exist for funding the RMS acquisition and installation. These options may be local, regional, state, and/or federal depending on the agency and where it is located. Funding options are addressed in more detail in section 3 of this report.

As part of developing the strategic plan, the available funding options must be identified, and preliminary contacts made with prospective funding sources so that the likelihood of adequate project funding can be assessed. The agency's financial management or contracting office should provide advice on applying for grants and requesting funding from other sources. The contracting office also should advise the agency regarding the point at which actual funding commitments must be made.

1.6 Organizational Commitment

Conversion to incident-based reporting and a NIBRS-compliant RMS impacts the way the agency does business. In addition, the transition requires extra effort on the part of many agency staff. For these reasons, the RMS replacement and the agency's conversion to incident-based reporting must have full support of the agency's top management. Management's commitment must be clearly stated, and employees' duties in RMS implementation and operation must be defined.

A statement of support for the project from an appropriate executive should be used to introduce the strategic plan. In smaller agencies, this could be from the Chief of Police or the Mayor; in larger agencies, this statement could be from a Deputy Chief. Regardless, executive level decision-making and active participation are crucial.

A key sign of support is the naming of senior law enforcement official or an experienced and trusted civilian employee as the NIBRS/RMS project manager. Ideally, the project manager leads the project planning and decision-making effort. However, some agencies may choose to name the project manager only after the project has been approved. The project manager must report to a top agency official, preferably the Chief of Police or a Deputy Chief of Police, so that supportive management actions are timely and assured.

Full support of and participation in the project by key agency personnel is very important. Ideally, the project team should be established across the organization so that all affected departments have input. The assignment of staff to the project team and to working groups should represent the divisions of the organization, which are most affected by the project.

1.7 The Decision

After the costs and benefits of the NIBRS/RMS project have been calculated, an approach defined, and potential funding sources identified, the agency can decide whether to proceed or not. This cannot be a half-hearted decision; it is a decision to fully commit an agency (and perhaps other government entities as well) and personnel to a substantial effort. The agency should be convinced that benefits out-weigh costs.

If the agency decides to implement a NIBRS-compliant RMS, it can proceed to involve the community. Some agencies may seek active community participation, while others may keep the community aware of the project and its likely benefits.

1.8 NIBRS RMS Decisions, Lessons Learned

The following list contains "lessons learned" and advice from state and local agencies that are NIBRS-certified or are implementing a NIBRS-compliant RMS. Agencies should reference this list for practical advice that can be used in conjunction with the activities specified in this section of the handbook. Comments from vendors of NIBRS-compliant RMSs have been included where appropriate. The comments in this list do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor communities.

Lessons Learned from Agencies:

- Don't be afraid to change things to get to NIBRS from the old ways of doing reporting/business . . . have an open mind.
- Keep all people/staff informed about NIBRS throughout the process in order to keep it on their minds (talk about it at every management meeting, give presentations and Q&A sessions, write a NIBRS article in the daily/monthly bulletin, hold preliminary classes/training).
- Acquiring and implementing NIBRS-RMS is the most complex project that the agency will ever do.
- Conversion to NIBRS is much easier if your agency and state already have incident-based reporting.
- State-level criminal justice system (including crime reporting) works well because local agencies cooperated in its development.
- Your planning needs to account for the fact that initially it takes a lot more officer time and more back office editing time as their learning curve

increases; it will level out, but still be more than what it was if you did Summary UCR before.

- Need full commitment from the Chief and his executive staff as well as other criminal justice leaders in the community—courts, prosecutors, sheriff, etc.
- City council must be prepared to see different (perhaps higher) crime statistics numbers so there is no negative reaction.
- The greater length of time that it takes to complete incident reports is offset by the agency getting a better look at crime.
- Substantial benefits in crime analysis and crime mapping.
- NIBRS produces better information and a more readable report.
- The computer can do a lot for you. Before NIBRS-RMS, record clerks had to read every report individually.
- When an agency compares the Summary report procedure to NIBRS', it must account for the fact that it takes longer to prepare an Incident Report, enter the data and back-end edit it—the Report is much longer and more complex (our old offense report was 1 page, now it is 8 pages).
- NIBRS forces better crime scene data collection and is better for reporting hate crimes. Better crime analysis.
- Questions by the officers when completing report show victim a higher level of caring.
- Talk with other agencies. Go onto the Internet.

Lessons Learned from States:

- Research!
- Every week in planning saves a year later on.
- Talk to other agencies.
- Combine with other agencies in county or region to obtain an NIBRS-RMS.
- It's a big decision and a lot of work . . . know why you want to do it and know what the benefits are before getting started.
- Each agency has a responsibility to its state, jurisdiction, citizens, and its own agency to ensure complete NIBRS data reporting.
- Must talk to other agencies . . . learn from what they did right and from what they did wrong.
- It seems to take about 9 months for an agency to adjust to NIBRS; after that, agencies seem to have adjusted and seem okay.

Vendor Comments:

- Agencies need to realize and accept that their culture will be changing with the new RMS.
- Top management as well as middle managers must buy into the modernization and openly support it.

Other Lessons Learned:

Top six reasons for successes are:[1]

- User involvement.
- Executive management support.
- Clear requirements.
- Thorough planning.
- Realistic expectations.
- Smaller project milestones.

[1] Standish Group, *The Chaos Report,* 1995

CHECK LIST FOR NIBRS RMS DECISION

- **Justify System Change:**
  - Define existing problems and how the NIBRS-RMS can address those problems.

- **Define Project Boundaries:**
  - **Goals.** What are the results of the project?
  - **Scope.** What are the system boundaries?

- **Estimate Approximate Cost of the RMS**

- **Address Operation and Maintenance Costs:**
  - O&M Options
  - Estimated Costs

- **Explore Funding Options:**
  - Which options are feasible?

- **Develop Strategic Plan:**
  - Document information

- **Get Organizational Commitment**

- **Make Decision**

- **Notes and Comments:**

2 DEFINE THE RMS

Once the decision to proceed is made, the agency must define the RMS to be acquired and begin preparing for the change to NIBRS and the new RMS. This section addresses RMS definition. Section 7, *Agency Preparation*, addresses the parallel activities of preparing the agency. The guidance is for agencies of all sizes. However, the level of detail to be included in the RMS definition varies depending on project's goals, funding sources, and acquisition strategy.

The RMS can record, store, retrieve, manipulate, view, and archive information relevant to the functions listed in Table 1.2. The RMS can capture information from mobile data computers (MDCs), computer-aided dispatch (CAD) system, and computers at other agencies such as the Sheriff's office, courts, and corrections. The RMS can also transfer information to those systems.

To define its RMS, an agency should:

- Designate the project manager and RMS team.
- Define the agency's functional RMS requirements.
- Define the system requirements and constraints.
- Define the RMS interfaces.
- Define the RMS operating environments.

2.1 Designate the Project Manager and RMS Team

The project manager should know the agency's organization, be respected, and be able to get results: an extensive technology background is not necessary. Ideally, the project manager should be appointed to lead the preparation of the strategic plan (see section 3). If not, the appointment must be made before the RMS definition begins. The project manager must have a thorough understanding of the agency's needs and priorities and how those are translated into system specifications and work statements. The best way of acquiring that information is to analyze the system requirements.

The project manager may need staff help, depending on his or her level of experience and the magnitude of the project. In larger agencies, the project manager will definitely need staff. The staff should include personnel who can help define and document the RMS requirements and deal with funding and acquisition issues.

For a small agency, a project manager will be needed—perhaps part-time—and a working group should be established. The extent of participation in the working group should be based on the size of the agency; however, the group should include someone who understands all aspects of the agency's operation that will be affected by the new RMS and NIBRS reporting.

Someone on the project team should be competent to assemble technical requirements, communicate with candidate system vendors, and prepare for system installation and transition. This person could be a consultant during the acquisition phase. However, once the system is operational, an agency will need a dedicated RMS manager who understands the business and technical aspects of the system and can help resolve operational problems. Preferably, this RMS manager should be part of the RMS project management team from the beginning. Continuity of staff is an important component for successful system transition.

Under the direction of the project manager, the RMS working groups must be established with a variety of knowledgeable members who represent each of the business areas affected by the new RMS. Agency management must allocate a significant portion of the working group's time to RMS definition activities so that the project's schedule is maintained and all needs are identified. The groups must be kept small enough to be effective, so there may be multiple groups with each assigned responsibility for a specific requirement. For a larger agency, the working groups should include the following representatives:

- **A Command staff** member should chair the working groups and ensure their effectiveness. This person should also represent the agency's system needs, e.g., administrative and statistical reports.
- **Patrol officers** are the source of much of the information needed for the system. They can provide guidance and opinions on the types of data to be collected and the impacts of various data capture approaches.
- **Case investigators** represent one of the major groups of users of the system and its information. They can discuss access needs and types of data they require.
- **Record personnel** enter data into the system, and they are responsible for preparation of accurate state and NIBRS reports.
- **Prosecuting attorneys** can address their specific needs for incident and arrest information in terms of content, timeliness, and accuracy.
- **Someone representing the courts,** including court calendars, offender identification, and dispositions. If this information exchange can be accomplished electronically between systems, clerical workload will decrease and data accuracy will improve.
- **Crime analysts** need access to fresh, thorough information on crime in geographic areas. Also, they may need computer support in their analyses.
- **Special areas** may need representation depending on the scope of the RMS being procured. For example, if a property management module is being acquired, then someone from property should participate.
- **Business processing staff** understand how the agency's business processes will be affected. They can help in assessing the needs, ensuring that they are consistent and coherent, transferring them into RMS specifications, and revising policies and procedures if necessary.

- **Technical staff** address questions such as communications, security, file conversion, interactions with other systems, site preparation, etc. Technical personnel may form a separate working group.

Some working group members will participate in RMS vendor selection (see section 4), and some may be part of the implementation team. (See section 5.)

2.2 Define the Agency's Functional RMS Requirements

Functional requirements define specifically what the RMS is to do. These requirements are defined by people in the agency who are familiar with, and/or responsible for, the law enforcement and criminal justice records management functions that may be affected by the new RMS and/or NIBRS reporting.

2.2.1 Types of Functional Requirements

The better the agency's functional requirements are collected and documented, the more likely it is that the new RMS will perform effectively. Extra time spent on this step will more than pay off in the successful implementation and operation of the RMS.

As an example of functional requirements, the RMS software product must be able to manage an agency's incident information. Specific RMS functions should record stores, process and report information, and provide easy on-line user retrieval.

Within major system functions, the agency may prioritize specific functional requirements as:

- **Mandatory.** The RMS must perform mandatory functions without exception. In evaluating competing RMS systems, the agency would not consider RMS products that did not perform this function. In the specification, mandatory requirements are designated by the verb "shall."
- **Desirable.** The agency would consider RMS products that did not perform desirable functions if the product did perform all of the mandatory functions. In the specification, desirable requirements are designated by the verb "should."

Table 2.1 is an example of how the recording of incident management information could be documented. The example is not complete; rather, it illustrates a format and process.

In key areas, agencies should be very specific about what they want. For example, most RMS vendors claim to be "NIBRS-compliant." However, some

agencies have found those claims to be questionable, at best. Agencies should specifically define what is meant by NIBRS-compliant, and document that as a mandatory requirement.

Another issue related to NIBRS compliance is compliance with an agency's state reporting requirements. Again, agencies should be specific in this area; however, since each state is different, meeting state reporting requirements may require extensive tailoring. The best solution to this is for agencies to ask their state program for the list of vendors who can comply with the state's reporting needs. Agencies should then make sure those vendors are invited to bid on their Request for Proposal (RFP).

Table 2.1 An Example of Functional Requirements for Incident Management—Data Capture

Requirement Number	Functional Requirement	Mandatory	Desirable
A.1	INCIDENT MANAGEMENT		
A.1.1	Capture Incident Data	X	
A.1.1.1	The system shall provide a capability to record all data elements currently contained on Agency Incident Report, Form No. I-1234.	X	
A.1.1.2	The system shall provide the ability to support the entry of multiple offenses for a given incident.	X	
A.1.1.3	The system shall provide the ability to relate a victim to one or more offenses.	X	
A.1.1.4	The system shall provide a means to record incident-specific data based on the incident classification entered by the officer. For example, a burglary incident report shall allow entry of indication of forced entry, point of entry, method, and tools used.	X	
A.1.1.5	The system shall provide a capability to assign more than one role to a given person involved in the incident. For example, an individual may be identified as both a victim and the offender for the incident.	X	
A.1.1.6	The system should provide the ability to record information for incidents requiring auto removal, including name of towing company and storage location of the automobile.		X
A.1.1.7	The system should provide the ability for the data entry person to record incident data such as address and name of complainant directly from the CAD system without having to reenter the data manually.		X
A.1.2	Store Incident Data	X	
A.1.3	Process Incident Data	X	
A.1.4	Support On-Line User Retrieval of Incident Data	X	
A.1.5	Provide Incident Reports to Agency Personnel	X	
A.1.6	Prepare NIBRS and State Crime Reports	X	
A.2	Arrest report creation/Arrest Data Capture		

2.2.2 How the Functional Requirements are Collected

Agencies of all sizes should define their functional requirements; and the extensiveness of those requirements will define the collection process.

Medium and Large Agencies. Working groups will be the primary source for defining functional requirements. Agencies that have recently installed a NIBRS-compliant RMS can provide a good basis for requirements, which were used by them. Caution must be used since each agency has some unique operational needs that may not fit with those of another organization. Although the functional requirements from another agency can provide a good checklist for the working groups, the specifics should be closely reviewed and applied accordingly. To reduce confusion and help the groups maintain focus the working groups should develop functional requirements prior to review.

For a small agency, the strategy could be to spend some time describing what would help the agency most. Discussions with officers and support staff will reveal areas that would increase officer safety and efficiency, and/or would reduce clerical workload. Meetings with agencies that have already installed a NIBRS-compatible RMS will help in this effort as well. Some of these agencies may have specifications that an inquiring agency can use as a basis for its functional requirements definition. Help is also available through the CJIS Division of the FBI, BJS, the Police Executive Research Forum (PERF), the International Association of Chiefs of Police (IACP) (e.g., the Law Enforcement Information Management [LEIM] Section), or SEARCH, Inc. The source selection process (see section 5 of this handbook) will involve reviewing how close the proposing vendors come to meeting the agency's *mandatory* and *desirable* needs.

Each working group should have a leader to oversee each major function (e.g., *Incident Management*) and sub-functions (e.g., *Capture Incident Data*). The working group members should then describe each step that must be accomplished (i.e., "enter all data elements currently contained on Agency Incident Report, Form No. I-1234"). Someone should record all statements and translate them into requirement for review by the working groups. It is important that each requirement is tested and the software's ability to meet the requirement must be fully assessed or evaluated prior to acceptance.

A set of functional requirements should be developed for each major function being automated (see Table 2.1 for examples). In large agencies, this could mean a separate committee for each major function. In medium-sized organizations, many of the same people will participate in the development of requirements for several major functions.

2.2.3 Make Sure Requirements Are Reasonable

In developing functional requirements, agencies may find it useful to have some preliminary discussions with vendors about what their products can do. Such conversations can be helpful in ensuring that the agency's mandatory requirements are, in fact, realistic. A word of caution is appropriate here. It is to the vendor's advantage to have agencies write functional specifications that can be met by only their product. Agencies engaging in these preliminary meetings should coordinate with their contracting office to ensure those vendor conversations do not compromise the upcoming source selection process. In these conversations, the agency should confirm that *at least* two vendors meet the mandatory functional requirements with their standard COTS products without software modification. The products will still need to be tailored for a particular agency (use the agency's name, the agency's form contents, etc.), but many COTS RMS products are designed to be tailored without having to change the basic software.

Unless absolutely necessary, agencies should avoid requirements that force the vendor to write special software to meet a few functional specifications. This customization will substantially raise the cost of the vendor's product. Further, these changes create problems in ongoing maintenance of the software. Most RMS vendors periodically come out with new software releases that make their products perform better. These releases will not upgrade customized software; an agency will have to pay the vendor to upgrade the customized part of their product.

Some large agencies may find that they have a number of unique mandatory functional requirements. There may not be two or more RMS vendors that can meet those unique requirements with their COTS products. In those cases, the agency needs to do a trade-off analysis to determine which course of action has the best cost-benefits ratio:

- **Scrub the requirements.** Are the requirements *really* mandatory? What is the operational impact of not meeting them? If only a few requirements mandate expensive customization, do benefits outweigh development and maintenance cost?
- **Acquire a COTS product and customize it.** In these cases, the annual cost for maintaining the custom software as part of the vendor's normal release cycle should be negotiated as part of the contract.
- **Acquire a software package from another police department.** On the surface, this appears to be a great solution: a free RMS. Unfortunately, there are concerns that must be raised. Chances are, if a COTS package does not meet an agency's needs, it is even more unlikely that a package designed specifically for another police department is going to meet them. This means customization may be necessary, which may be acceptable if there is adequate documentation of current modules and systems and if

none of the software is proprietary software (i.e., property of a software developer). In either case, an agency will not be able to count on new releases to correct problems. Once an agency makes changes to the software, it becomes the agency's unique package.

- **Develop a unique RMS package.** Some developers will argue that with modern database management systems combined with secure Internet development capabilities, this may be a competitive alternative if an agency's requirements are truly complete. This approach requires a very competent in-house information technology (IT) department and a competent development contractor. When estimating development costs, software developers frequently underestimate the time it takes for the new system to become truly operational. Agencies considering this approach can develop an independent cost estimate for development of their unique RMS using the cost model described in section 3 of this handbook.

2.2.4 Document the RMS Functional Requirements

The *functional requirements* will become part of an agency's RMS specifications for the RMS applications software. These specifications, in turn, will become part of the contractual documentation with the vendor. For this reason, they must be carefully written so that they are unambiguous and contractually binding. For example, each requirement should be separately expressed and numbered. Table 2.1 shows example documentation of functional requirements. See section 4 of this handbook for more information on source selection.

In key areas, agencies should be very specific about what they want. For example, most RMS vendors claim their systems are NIBRS-compliant. However, some agencies have found those claims to be questionable, at best. Agencies should specifically define what is meant by NIBRS-compliant and document that as a mandatory requirement. Another issue related to NIBRS compliance is an agency's state reporting requirements. Again, agencies should be specific in this area. However, since each state is different, meeting state reporting requirements may require extensive tailoring. The best solution is for agencies to ask their state-reporting agency for the list of vendors that comply with the state's reporting needs. Agencies should invite and encourage those vendors to bid on their RFP.

People in the working groups should be allowed to express their thoughts freely, and they should not be burdened with describing the needs in specification format. A technical person from the project staff or a consultant can complete this task separate from the working group meetings.

2.3 Define the System Requirements and Constraints

System requirements address those properties of the RMS that are more-or-less behind the scenes of the software applications (which pertain to the *functional requirements)*. The system requirements consist of the following areas:

- Security and data access.
- User interfaces.
- System architecture.
- System administration.
- System performance.

An agency should not try to identify specific hardware or software packages or features that lead to specific packages. Instead, the agency should assume that the working groups are developing a "performance-based" specification. That is, the specifications should describe *what* the agency wants the system to do but not *how* it is to be done by the system architecture.

Agencies should check with city, county and/or state officials regarding any information system policies, standards, guidelines, and/or requirements that might exist and with which agencies might have to comply.

As with all RMS requirements, system requirements from other agencies that have recently installed a NIBRS-compliant RMS can provide an agency with a good basis for developing its own system requirements. There should be very few unique system requirements, so the ability to use them directly, if they are complete, is much higher than it is with the functional requirements. However, the agency should ensure that the specifications are performance based, not design-specific, and that each requirement is testable.

2.3.1 Security and Data Access

Security and data access requirements address the entire range of RMSs and how the integrity of the information will be maintained.

For a small agency, asking for as many of the following features as possible during vendor source selection is recommended.

For larger agencies, particularly those that are planning to have any form of Internet connection or those that are planning to connect to systems outside the agency, security will be more challenging. Some capabilities may be offered by the operating system provided by the vendor; others may be a part of the vendor's product line already. Below are the specific areas that should be addressed:

- User identification and authentication.
- Authentication policies and procedures.
- Authorization of remote access locations.

- Protection against message alteration.
- "Firewall" protection against external unauthorized access or attack from the Web.
- Virus protection.
- Protection against access by unauthorized personnel inside the agency.
- Detection of intruders.
- Screen-saver passwords and automatic timeout for logins.
- Classes of users so that not all system users have access to all information.
- Protection of juvenile records, internal investigation records, and other sensitive records.
- Logs of all transactions with ability to retrace all events by authorized auditors.

For small agencies that do not plan an Internet connection, the main concern will be to ensure there are passwords, including password-protected screen savers, which prevent an unauthorized person in the operations area from entering the system. Password protection should be provided by the vendor as part of the operating system and user interface. For example, if the vendor uses Microsoft Windows™ for its system, the basic capability will be provided. Also, there should be some capability to protect juvenile or sensitive records so that only authorized staff can access them.

2.3.2 User Interfaces

An agency will want a system that provides what is known as a user-friendly interface so that data entry and data access are easy to perform. Since "user-friendly" is a very general term, it will be necessary to be more specific in the RMS specifications. Specific terms that can be used for a computer terminal interaction include:

- **Graphical User Interface (GUI).** The MS Windows user interface guidelines can be referenced in the specification for this feature.
- **Prompting.** The computer provides the user with guidance on what to do next; for example, in entering an incident report, the RMS may prompt the officer to describe what was stolen, whether there were witnesses, etc.
- **Pull-down-menus.** These provide the user with a list that can be referenced so that when a match is found, the user only needs to "click" on the correct item; for example, in a robbery, a pull-down menu could list the different types of stolen property.
- **Touch screen entry.** Rather than using a drag and click mouse entry, the screen could be touched to select the correct item when there is multiple choice.
- **On-line help capability.** This is essential.
- **Pre-fill and automatic-fill.** For some fields such as date this is be a real time saver. If the system accepts data from the CAD system, then pre-

fill could also include complainant name and address as well as other information for officer approval and acceptance.

- **Data entry validation.** This helps to ensure data quality. It also saves time because errors are corrected while the incident and details are still fresh in the officer's mind.
- **Single entry of data.** Once they are entered, data become available for all RMS functions and do not have to be entered a second time.

There may be significant differences among vendors in this area, so even small agencies may want to include some user interface needs. There are some new technologies that may allow even easier data entry and inquiry. Voice entry and response technology has progressed very rapidly in the past few years. The vision of an officer at an incident with a headset verbally recording information is a real possibility for the future. This kind of technology can be included in the specification as a desirable rather than a mandatory requirement.

Other user interface requirements can deal with giving the user the ability to do multi-tasking, for example, making an inquiry while in the process of preparing an incident report.

2.3.3 Architecture Requirements

In general, the agency should not try to specify the computer hardware and system software (specific operating system, specific database management system, etc.). Agencies should, however, confirm that RMS architectural requirements conform to local and state government IT policies and standards, if any. Otherwise, the computer hardware and system software specifications should be left to the vendor.

There are some characteristics, however, that the agency may want to include in the system. These characteristics will increase the flexibility and adaptability of the system so that in the future the system can accommodate changes such as:

For a small agency, someone in the agency should be trained to perform system administration functions.

- Adjustments to the way the agency does business. New reports may need to be generated by the RMS, and new data may need to be accepted.
- New RMS sub-systems. For example, MDCs may be purchased by the agency, and these would have to interact with the RMS.
- Additional automatic exchange of information with other criminal justice systems such as courts and corrections.
- New technology (e.g., voice data entry).

Some key requirements that are important for both small and large agencies to consider can be documented by the following phrases:

- Capability to tailor screens or displays including adding or deleting fields, modifying field edits criteria, etc. without having to modify existing software or create new software.
- Capability to tailor reports, including creating new reports or deleting existing reports, using a report writer.

For larger agencies and smaller agencies desiring a network or Internet access, key phrases that should be considered include:

- Support of an open architecture.
- Use of standard SQL and relational DBMS.
- Implementation with two or more tiers (client/server architecture) that separates the GUI logic from processing and data storage.
- Support a Web-based interface.
- Support interface to a standard local area network. (If the agency already has one, then it should be specified.)
- Modularity of software so that the agency is not required to use modules that implement functions performed by external systems or agencies.

For a small agency, the items listed in section 2.3.3 should be included as requirements. Additionally, other items listed in section 2.3.3 should only be included if the agency is interested in a networked environment or Internet access, in which case, all items should be included.

2.3.4 System Administration

Business computer systems require a system administrator. For small agencies, this may be a person provided by the vendor or an outside contractor on an as-needed basis. For larger agencies, this may involve a part-time person or even a full-time staff, depending on the size of the RMS computer operation.
The RMS must support the system administrator by providing capabilities that (1) supply information on the RMS operation through system administration reports and (2) facilitate administrative functions.

2.3.5 System Performance

System performance refers to the speed, accuracy, and reliability with which the RMS performs its functions. It is important that an agency specify the level of performance it expects to have from its RMS. System performance is affected by:

- Volume of work that the agency processes on the RMS.
- RMS software.
- Processor upon which the software operates.

- Competing traffic from the local network and remote locations.
- Responsiveness of systems with which the RMS is integrated (e.g., court and correction systems).

Workload. Agencies must provide projections of expected workload and number of concurrent users. These projections should cover the first several years of operation. Typical information needed by the vendor includes:

- Number of names and addresses on file currently.
- Number of annual and seasonal incident reports. (If the agency is in a summer resort area, for example, and 90 percent of incidents occur in a 10-week period, that information is also necessary.)
- Number of annual arrests.
- Number of sworn officers.
- Number of years in which on-line database access to records is required, i.e., years before records are archived.
- Activity for other optional applications. (For example, if the agency is acquiring the property management module along with the RMS, then it should state how many items are currently in the property inventory.)
- Expected growth profile for the area in the next 10 years. (The Chamber of Commerce can probably provide statistics to use as the basis for this forecast.)
- Number of concurrent users (see below).

Number of Concurrent Users. Some vendors price their products based on the "number of seats," or concurrent users, referring to the maximum number of officers and staff that are likely to access the system at the same time. An agency should give careful consideration to this number. If it is set too low, the system will have insufficient capacity. Officers and staff would then have to wait for others to logoff before they could logon. On the other hand, an agency does not want to over-estimate the number of concurrent users, since this may unnecessarily increase the cost of the system. In most cases, additional "seats" can be licensed at additional cost after the system is operational, but there may be performance implications.

In calculating the number of concurrent users the agency should consider the maximum number of officers on duty during each shift and the frequency with which they will access the system. The agency should also consider the impact of the new RMS on operations. For example, adding MDCs that allow officers to enter searches on suspects

For a small agency, system performance should not be an issue unless the agency plans to have significant MDC access; even then, it is unlikely that the system will get overloaded. Small agencies should assume that their system will operate with a single processor, but they should plan to operate with printouts of key information in case the computer system fails for any reason.

and vehicle license numbers from their patrol vehicles may substantially increase the number of inquiries. Other considerations are the number of other staff who may be accessing the system and inquiries that may come into the system from other agencies. For larger agencies, a consultant or experienced computer systems engineer may be able to help make this calculation. Suggestions from other agencies can also help.

The agency's strategy could be to incorporate the current year's projected number of concurrent users into the specification, but indicate that the RMS must be able to accommodate growth in increments of, for example, 25 users when required. The cost of these incremental additions should be taken into account in the Statement of Work (see subsection 4.3.1).

Performance Goals. These goals should be operationally based (as observed by system users); not computer based and should reflect what the agency would find acceptable in RMS operation. Table 2.2 contains some examples of performance goals.

Table 2.2 Performance Goal Examples

Example Transaction Types	Example Response Times
Respond to report inquiry	Up to one second
Respond to name and address file inquiry	Up to two seconds
Display drop-down file information	Up to one second
Respond to archive inquiry	Up to thirty seconds
Database searches with indexed data	Up to three seconds
Response to MDC inquiries	Up to five seconds including communication time

These numbers are examples only and do not include time of the user in preparing the inquiry on the workstation or MDC. Also, no system will be consistent under all workloads, so the number should be expressed in a format such as "up to one second response 90 percent of the time, with response time never over ten seconds." If the response time goes over 10 seconds, the system is considered "not available." Response times could be expressed as desired goals, but then the agency will have no contractual basis for protesting poor response time.

System Availability. This describes the percent of time that the system is to be available to perform work. It is expressed as a percentage of time available versus total clock time. If the system were always available, the system availability would be 100%; however, it is unrealistic to expect this with any system even those used in manned space exploration. Availability is calculated as follows:

$$\text{Availability} = \frac{\text{System Uptime}}{\text{System Uptime} + \text{System Downtime}}$$

Downtime in this formula includes things for which the system vendor is responsible such as maintenance, system failures, and switching from a primary computer to its backup system.

Downtime *does not* include times when the RMS is not available due to reasons beyond the vendor's control such as power outages, disruptions in the computer room environment (e.g., air conditioning failure), or failure of a network that is not supplied by the vendor.

The higher the system availability number the agency specifies, the more expensive it becomes to meet. Following are two examples of how reliable the RMS should be:

For smaller agencies, the reliability measured will be that of the processor configuration. However, the reliability measurements must include everything in the processor configuration that was supplied by the vendor, such as the printer.

- **99.0 Percent.** In a 24 x 7 operation, if a computer has a system availability of 99%, it would have on average no more than 15 minutes of downtime every 24 hours. With today's computer systems, a single processor computer system should be able to meet this figure. An agency may also want to specify a maximum length of downtime for any single downtime event (e.g., one hour). For example, if the RMS system failed only once during the year, but the failure lasted for 84 hours, it would meet the 99% availability requirement even though it might be disastrous for the agency's operation.
- **99.9 Percent.** If an agency were to specify a system availability of 99.9%, the vendor would be forced to use a dual processor and the system would probably require 24-hour on-site maintenance. The failure of one of the processors might mean degraded response time, but the system would remain operational. Larger agencies may be able to justify the dual processor configuration; however, smaller agencies would likely find the higher availability to be quite costly.

Agencies should discuss their projections of system availability with different RMS vendors and, in the light of the agency's needs, arrive at a reasonable availability figure.

Larger agencies may have a complex system in which the RMS configuration is only one part. In such cases, the availability of the overall system must be considered. To reach the RMS and MDC, a transaction must travel through several system components. Suppose these components have the following levels of availability:

- RMS, availability = 99.0%
- MDC, availability = 98.0%
- MDC-to-RMS communications link, availability = 95.0%
- MDC switch in the computer center, availability = 99.0%
- Local area network in the computer center, availability = 99.0%

In these circumstances, the availability for any given MDC to connect to the RMS is 90.3%. If the RMS availability were increased to 99.9%, the MDC connection availability would increase to 91.2%. Specifying higher RMS availability, in this case, only slightly improves overall MDC-to-RMS connection availability. Overall, the agency should consider system availability needs of all users, as well as the cost and benefits of higher requirements.

2.4 Define the RMS Interfaces

Agencies must specify the interface to each system with which the RMS will be expected to communicate. For small agencies, this could be as simple as a dial-up connection to the state NCIC 2000 switch, if there is any external connection at all. For larger agencies, those interacting with other agency systems (e.g., MDC system, Automated Fingerprint Identification System, property system, personnel system, etc.), each interaction must be described. The more information provided to the vendor, the more accurate and fixed the vendor's price will be. Below are two sample options for dealing with interfaces. These examples represent two ends of a range of available options:

For a small agency that plans to operate on a stand-alone personal computer, this will be fairly straightforward. The vendor must know if the agency plans to place the computer in a normal office environment. If not, the agency must describe the physical space in which the processor is to be located. If the computer is to connect to the state switch or any other system, the communications link must be described. In many cases, this will be the common carrier telephone line. The vendor will indicate if the computer requires any other support.

- **Broad Definition.** Generally, the agency should describe the interface, the kinds of information that will be exchanged, and how. For example, "All connections to the RMS shall be through the agency's local area network, which is a [name the type of network]. There shall be a connection to the Department of Motor Vehicles (DMV) to access registration and driver permit information." In this case, the vendor would probably respond with a time and materials proposal for preparation of an interface control document (ICD). This cost would be in addition to the cost of actually implementing the interface in the RMS.
- **Specific Definition.** Prepare an ICD. The ICD must be negotiated between the agency and the DMV in this example. The ICD must contain a detailed description of the inquiry transaction that is sent to the DMV and a detailed description of each response that may be received. Any

difficulties that the vendor encounters in establishing the interface that can be attributed to errors in the agency ICD will likely entail additional time and materials costs to the agency.

If access to the system is through the Internet or through a local area network, then the specifics of how the system is to connect to and interact with these networks must be described.

2.5 Define the RMS Operating Environments

If the RMS vendor is providing new processing equipment to an agency as part of its contract—or if the agency is acquiring new processing equipment separately—then the vendor will want specifics about the facility and the environment into which the processor configuration is to be placed.

For medium to large agencies, the vendor must know the following kinds of information.

2.5.1 Communications Links

If the processor is to communicate with other processors or remote personnel, then each communications link to be used must be described, including the local area network. The network vendor can provide a description of its connections, including protocol, speed, cable connectors, etc.

2.5.2 Computer Location

If an agency plans to locate the new RMS processing suite in an environmentally-controlled computer room along with other systems, the operating environment of the room should be stated. This could include operating temperatures, backup and/or uninterruptible power source (UPSs) that would be separately supplied, space restrictions for access space to cabinets, and conditions for rack mounting.

2.5.3 Existing Work Stations

If an agency already has, or plans on separately acquiring, work stations that will be used to access the RMS processing suite, the hardware configuration and operating system(s) of these work stations should be specified. This will include type, size, speed, operating system release, and network access software.

2.6 Source Selection

Once the RMS system has been adequately specified, the source selection process can begin. This process is described in section 4 of this handbook.

2.7 RMS Definition, Lessons Learned

The following list contains "lessons learned" and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Agencies should refer to this list for practical advice that can be used in conjunction with the items specified in this section of the handbook. Comments are from NIBRS user and vendor communities and from NIBRS-RMS vendors, where appropriate.

Lessons Learned from Agencies:

- Don't be afraid to change things to get to NIBRS from the old ways of doing reporting/business . . . have an open mind.
- Keep all people/staff informed about NIBRS throughout process in order to keep it on their minds (talk about it at every management meeting, give presentations and Q&A sessions, write a NIBRS article in the daily/monthly bulletin, hold preliminary classes/training).
- PLAN, PLAN, and PLAN.
- Acquiring and implementing NIBRS-RMS will be the most complex project that the agency will ever do.
- Explore your options—depending on the complexity of your requirements and your staff, in-house development may be attractive.
- Spend time designing the offense report to get it right—we spent 2 years.
- Use of MDC with pull-down menus, prompting, and on-line editing should reduce time for NIBRS-compliant report preparation by 50%.
- Need a teamwork philosophy across the agency. A teamwork philosophy is needed across the agency.
- Get all users involved up front.
- A business practices team needs to revise procedures and redesign forms.
- Remember that contractors cannot solve all your problems. Everybody needs to immerse himself or herself in what NIBRS is all about (really get to know what it provides and why to do it).
- Understand the system.
- If you spend 18 months planning, then you can do a 6-month implementation; if you spend 1½ hours planning, then you'll spend 18 years implementing.
- Need a full-time advocate.
- Get the right people involved . . . must have Vision.
- Don't have a person in charge who is frightened about change; [NIBRS] requires a leader who believes in the process/project and can instill this in others.
- Don't build into a dead-end situation.
- It is a long, tedious process, so treat it that way from the beginning . . . "[The] devil is in the details."
- Spend lots of time in preparing a detailed RFP . . . a vague RFP leads to drawn out negotiations; we should have put more detail in our RFP.

- Must have a spokesperson that keeps this issue out in front of everyone.
- Include actual, real users in the process.
- Dedicate staff to the team full-time, and include staff/input from all impacted users (e.g., courts).
- Need PR within your agency.
- Prepare as much as possible.
- Get your data structured BEFORE you start (tables, codes, mappings).
- Make sure that your agency is classifying crimes correctly in Summary, before moving to NIBRS. Otherwise, comparisons of crime rates will be "apples to oranges."
- Start researching for NIBRS early. PLAN!
- A small agency should research for 1 year before starting [the] acquisition process. A large agency (250,000+ population served) should research for 3 years before starting.
- Take a "NIBRS for dummies" approach as best as you can. Simplify.
- It may be more effective for an agency's management to require "NIBRS or else" in order for the ranks to adapt.
- Acquire the latest technology.
- Make [the] RFP very specific in what you want.
- Must create NIBRS experts within your agency.
- Pay attention to how the program puts the data into the RMS. Ensure proper user interface flow, from input to storage to reporting.
- Look closely at the need for custom programming; will it be covered by the maintenance agreement?
- Talk with other agencies. Go onto the Internet.
- Make sure officers, staff, and management are working together toward the common goal.
- Nothing moved forward with a committee of part-time people. Implementation was done by one full-time person [agency has 50 sworn officers]. Did not start until the last minute, so participation by officers and staff was minimal; this created problems of acceptance.

Lessons Learned from States:

- Research!
- Every week in planning saves a year later on.
- Talk to other agencies.
- Assemble a committed staff/team.
- Spend a lot of time on defining requirements/needs . . . BE VERY SPECIFIC.
- Get input from your customers . . . in other words, from agencies throughout your state.
- Must manage people well, make sure all on same page.
- Dedicate resources [and] staff to RMS processes.
- Identify your own needs first.

- Make absolutely sure that hardware (existing or new) is compatible with the software.
- Know what you want to get out of the system.

Vendor Comments:

- Make sure the state trains the agencies on their reporting demands and that these demands are included in the RMS specifications so that the new RMS software does not get blamed when the reporting is wrong.
- Data entry people must be trained—they can't make as many errors as they might have with Summary UCR report preparation. Edit checks in the software help to catch some mistakes.

CHECK LIST FOR RMS DEFINITION

- **Designate Team:**
  - **Project Manager** Designate during *strategic plan* development
  - **RMS Team** Get representatives from areas that will be affected by the new RMS and NIBRS

- **Define Functional RMS Requirements:**
  - **Mandatory** Must be performed by the RMS
  - **Desirable** Might be performed by the RMS, but not required
  - **Set up Working Groups** Provide "straw man" requirements and assign leader to each group
  - **Check Reasonability of Requirements**
  - **Document RMS Functional Requirements in RMS Specification**

- **Define System Requirements:**
  - **Security and Data Access** User authentication, authorizations, etc.
  - **User Interfaces** Graphical User Interfaces, prompting, etc.
  - **System Architecture** Multiple tier system, modular, etc.
  - **System Administration** Support for system administration
  - **System Performance** Speed, dependability, etc.
  - **External System Interfaces** Interactions with other systems

- **Define External System Interfaces:** Include all systems that are to communicate with the RMS

- **Define the RMS Operating Environment:** Include power supplies, heating, etc.

- **Complete the RMS Specification:** Capture all requirements in the RMS specification

- **Notes and Comments:**

3 DEVELOP COSTS AND FUNDING SOURCES

This section addresses how an agency can estimate the cost of acquiring a NIBRS-compliant RMS and describes other cost and funding considerations.

A cost model developed for the FBI and BJS is available to agencies for estimating RMS costs. This model and its use are described in section 3.1 below; a user guide is provided in Appendix C. Additional cost considerations such as purchase versus lease, use of existing contracts, and total life cycle costs are addressed in section 3.2. Section 3.3 addresses potential federal funding sources for agency RMS acquisitions.

3.1 Cost Model Description

A cost model was developed to project costs associated with the implementation of a modern NIBRS-compliant RMS. Costs may be projected for different levels of automation and for different sized law enforcement agencies. The model includes an analysis of the gross costs of implementing the automated NIBRS-compliant RMS. The following are categories of costs from the cost model:

- Hardware.
  - RMS server and accessories.
  - User equipment.
- Software.
  - RMS.
  - Database licenses.
- Training.
- Installation.
- Data Conversion.
- Annual O&M.

Agencies should recognize that many factors determine the cost of their RMS. The number and types of system modules, the complexity of networks, and many other factors shape both the scope of the RMS and the cost of the entire system. The cost model described in this section addresses only those cost factors associated with acquiring a NIBRS-compliant RMS. RMS vendors offer many useful modules (e.g., CAD) that agencies may want or need. However, the cost model does not help in estimating these additional costs. For many agencies, the acquisition of a NIBRS-compliant RMS is only one part of an overall technology upgrade. Even though it is important for agencies to determine the cost of their entire IT project, this cost model helps estimate the cost of only the NIBRS-compliant RMS part of the project.

This model assumes that the technical sophistication of a given agency, which is not currently capable of reporting NIBRS data, would be at one of three levels:

- No existing RMS.
- A non-incident-based RMS.
- An incident-based RMS.

The cost model is an interactive Excel™ spreadsheet requiring a few externally supplied parameters specific to the subject agency. A detailed description of the cost model may be found in Appendix C and in the *Cost of Implementing & Operating a NIBRS Capable Records Management System*, dated June 14, 1999. For further information on the 1999 report, contact the FBI or BJS.

The scope of this effort encompasses only those components necessary for the implementation of a NIBRS-compliant RMS. It does not address such information system components such as file and print servers, E-mail systems, and Internet access devices. There are cases where the use of the cost model is not appropriate to the task of identifying costs for a given agency. These cases typically involve agencies that are either able to add NIBRS reporting capabilities to their existing RMS with minimal modification or outside the scope of the model in terms of size.

3.1.1 Global Assumptions

The following global assumptions were created in order to qualify the scope of the cost model in terms of input parameters and output results. These assumptions are the result of information gathered through interviews with NIBRS-capable RMS vendors and with law enforcement agencies.

1. The model produces "Class B" cost estimates in the approximate range of +/- 25%.

   Mitretek's Business and Economic Analysis Center uses the term "Class B" estimate to identify an estimate that averages the prices from several vendors in order to obtain the basis cost relationship between the number of concurrent users and the total cost of user licenses. The estimate is based on real world data, but there are variances on how vendors price their individual products.

2. The model estimates the cost of a NIBRS-compliant RMS without state or local modifications.

   All 53 elements of NIBRS are consistent across all COTS products supplied by vendors of NIBRS-compliant RMSs. These 53 published NIBRS elements can also be used in performing a function point analysis of the level of effort required to create a NIBRS-compliant RMS. Due to the variation in the availability and costs of state and local specific Incident-Based Reporting (IBR) System modules supplied by vendors

and the varying complexity of each state's reporting requirements, these specific modifications were not incorporated into the model.

3. The model requires some outside analysis.

   Some analysis outside of the model may be required in order to determine the values of the input parameters, e.g., the number of additional workstations needed for the NIBRS-RMS and the number of remote sites that have insufficient wide area network (WAN) connectivity to support using NIBRS. Some changes may result from re-engineering existing reporting processes to accommodate NIBRS. The impact of these changes must be determined before using the cost model.

4. The NIBRS-Compliant RMS costs are for a "core" system without add-on modules.

   Cost estimates include only those items that can be considered "core" or "base"components of a NIBRS-compliant RMS. Modules such as CAD, crime analysis, permit processing (e.g., bicycle, handgun, etc.), shift bidding, and vehicle maintenance are not included in this study because of the large variation in vendor offerings, costs, and agency-level custom tailoring. It should also be noted that aside from an integrated CAD system's ability to enter header information (e.g., date, time, location) into a new report, these modules typically have little or no impact on the generation of monthly NIBRS reports for transmission to either state or federal authorities.

5. The model is not applicable to very large agencies.

   Cities with more than 1,200 sworn officers may require specific analysis due to their diverse and complex nature. Large cities typically incorporate a high level of specific custom tailoring in order to meet requirements generated by policymakers and law enforcement personnel. These variations cannot be generically modeled with the level of accuracy required for this effort.

6. Components from other systems are not reused.

   The ability to calculate the capabilities of an existing system component, such as a server hosting a CAD system or an older RMS, falls outside of the scope of this cost model because of the subjective nature of the existing system's processing and data storage expandability and the costs associated with required upgrades (i.e., upgrading a Compaq sequent symmetric multiprocessor [SMP] platform versus a Sequent SMP

platform). Each system component would have to be evaluated on a case-by-case basis in order to determine its suitability to the task of supporting a new RMS.

7. The model does not estimate costs for re-engineering report forms.

   Re-engineering report forms is a business process requiring each agency to determine the method in which its officers will record and transmit crime related information (i.e., forced choice report forms, narrative report forms, automated field reporting, dictation, etc.). Also, each state and local agency's reporting requirements—with regard to the number of specific IBR elements and additional text and information fields—vary too greatly to be modeled within the accuracy range of this effort.

3.1.2 Cost of Implementing a NIBRS-compliant RMS

Agency size provides the basis for estimating the cost of implementing a NIBRS-compliant RMS. The initial research of product vendors indicates that there are no universal definitions associated with the agency size. The status of the agency's information technology infrastructure after implementing a NIBRS-compliant RMS provides the following sizing definitions used in the model:

Small: stand-alone computer only.
Medium: local area network (LAN) with multiple workstations.
Large: wide area network (WAN) connecting multiple LANs (usually precincts or districts within a large jurisdiction).

In addition to agency size, there are two key sets of parameters used to generate cost: internal parameters and agency-specific parameters.

Internal Parameters. A set of internal parameters has been entered into a spreadsheet within the model. These parameters can be viewed by the user, but are password-protected against change to ensure the consistency and integrity of the internal parameter. These parameters are based on information collected from vendors and agencies and are described in detail in the cost model and its documentation. The types of internal parameters are as follows:

- NIBRS-RMS Software: unit cost of a staff month, cost of NIBRS-RMS SW licenses, unit cost of a filed mobile server license, unit cost of a filed mobile laptop license.
- Database Software: base cost of software license, cost of additional concurrent user licenses.
- Hardware: unit cost of RMS server, unit cost of desktop, unit cost of laptop (standard and ruggedized), unit cost of router, unit cost of printer, unit cost of network hub.
- Training: cost of training a class, cost of training one student.

- Installation: unit cost for installation of cabling and wall ports, initial cost of circuit installation.
- Data Conversion: one-time cost of data conversion (function of agency size).
- O&M (hardware and software): cost-estimating ratio to provide support on a 8 x 5 basis, cost-estimating ratio to provide support on a 24 x 7 basis.
- Other Parameters: average number of work days per month, average number of working hours per day, average number of incidents entered per hour by data entry clerk, percent of sworn officers making concurrent queries, concurrent user escalation factor.

Agency Specific Parameters. Each agency enters agency-specific data, which is composed of the following:

- **Initial state of agency.** No RMS, non-IBR RMS, or IBR RMS.
- **Agency design solution.** COTS or custom.
- **Help desk requirement.** 8 x 5 or 24 x 7.
- **Multi-user.** Yes (for LAN or WAN) or no (for stand-alone system).
- **Sworn officers.** Number of full-time-equivalents.
- **Connectivity or bandwidth.** Number of remote sites requiring new connectivity or additional bandwidth for NIBRS-RMS.
- **Participation.** Number of remote sites participating in NIBRS-RMS.
- **Incidents.** Number of NIBRS incidents per month.
- **Workstations.** Number of additional workstations needed for the NIBRS-RMS.
- **Printers.** Number of additional printers required.
- **Field reporting required.** Yes or no. If yes, enter:
  - Number of concurrent mobile users.
  - Number of additional standard laptops needed for the NIBRS-RMS.
  - Number of additional ruggedized laptops needed for the NIBRS-RMS.

The cost model is able to estimate the cost of a variety of scenarios and sizes along a continuum. Table 3.1 contains agency-specific parameters and results for twelve different scenarios. Parameters not included are valued at zero. A discussion of the scenarios follows.

Small Agency. The cost for the three scenarios for Small Agency—**no RMS**, **non-IBR RMS**, and **IBR RMS**—all have the same cost estimates. This is based on the assumption that a small agency will choose a COTS solution, since it is likely that the agency does not need the capabilities of a custom solution. Also, since a small agency will have a stand-alone computer, the cost will not vary with changes in the number of sworn officers or in the incident rate. In each of these scenarios, an agency would buy a single-user COTS solution.

For a small agency with either an existing **non-IBR RMS** or with an existing **IBR RMS**, the assumption is that the agency would replace its current RMS with a new single-user COTS solution that is NIBRS-compliant. This practice avoids the expense of data conversion. The agency normally would not have access to the source code to modify the existing system, and it would be too expensive to hire a contractor to make the modifications.

Medium Agency. For the three scenarios involving medium-sized agencies, the number of sworn officers and the incident rate remain the same regardless of the agency's current RMS. A COTS solution is assumed. The variance in cost is due to changes in the amount of equipment procured.

For the scenario with **no RMS**, cost estimate for 10 additional workstations and 20 laptops was included. The cost estimate for the medium agency with **non-IBR RMS** scenario assumes that there are some workstations that will be reused. The number of mobile computers was reduced. These changes were made in order to demonstrate the ability of the model to handle different equipment options. The cost of an **IBR RMS** COTS solution is equal to the cost of a **non-IBR RMS** COTS, so this scenario is not shown in Table 3.1. Instead, the cost estimate for the medium agency **IBR RMS** scenario illustrates an agency that contracts with a software developer to produce a custom modification in order to make the existing system NIBRS-compliant. The equipment profile was held constant from the **non-IBR RMS** scenario in order to demonstrate the impact of going to a customized solution.

Large Agency - COTS Solution. For the scenarios involving large-sized agencies, the number of sworn officers and the incident rate remain the same. There are 100 mobile users and ten remote sites included. A COTS solution is illustrated for the first three. The variance in cost is due to changes in the assumptions about the amount of equipment procured.

The cost estimate for the large agency with **non-IBR RMS** scenario assumes that some workstations will be reused, and the number of mobile computers was reduced. Again, these changes were made in order to demonstrate the ability of the model to handle different equipment options. The cost estimate for the large agency **IBR RMS** scenario is the same as the COTS solution cost for a **non-IBR RMS** scenario.

For the scenario with **no RMS**, 10 additional workstations and 20 laptops were included in the cost.

Large Agency - Custom Solution. Three additional scenarios for large agencies illustrate the cost of custom software development. The dominant cost factor is the expense of the custom code, when compared to large agency COTS solution costs.

The variation in cost among large agencies is due to changes in the assumptions about the amount of equipment procured and the use of custom software development in place of COTS. The **no RMS** scenario assumes higher quantities of equipment are required than the other two scenarios. With **no RMS**, it is assumed that the entire system will be replaced with no reuse of existing software. The large agency **non-IBR RMS** scenario assumes that some of the code from the existing system will be reused than **non-IBR RMS**. The cost is therefore reduced even further. The equipment profile for the **non-IBR RMS** and **IBR RMS** cases have been reduced from the **no RMS** scenario.

For further information on how to use the cost model to project costs, see Appendix C.

Table 3.1 Cost Scenarios							
Size		**No RMS**		**Non-IBR RMS**		**BR RMS**	
SMALL		Design Solution:	COTS	Design Solution:	COTS	Design Solution:	COTS
Stand Alone		Adtl Workstations:	0	Adtl Workstations:	0	Adtl Workstations:	0
		Adtl Printers:	1	Adtl Printers:	1	Adtl Printers:	1
Help Desk:	8 x 5	Adtl Laptops:	0	Adtl Laptops:	0	Adtl Laptops:	0
Multi-User?	No	Rug'edzd Laptops:	0	Rug'edzd Laptops:	0	Rug'edzd Laptops:	0
Field Reporting?	No	Hardware:	$3,079	Hardware:	$3,079	Hardware:	$3,079
Sworn Officer:	10	Software:	$4,521	Software:	$4,521	Software:	$4,521
Remote Sites:	0	Training:	$598	Training:	$598	Training:	$598
Incidents per Month:	100	Installation:	$1,061	Installation:	$1,061	Installation:	$1,061
Concurrent Mobile	0	**Total:**	**$9,259**	**Total:**	**$9,259**	**Total:**	**$9,259**
User:		**O&M:**	**$758**	**O&M**	**$758**	**O&M**	**$758**
MEDIUM		Design Solutions:	COTS	Design Solutions:	COTS	Design Solutions:	CUST
Local Area Network		Adtl Workstations:	10	Adtl Workstations:	1	Adtl Workstations:	1
		Adtl Printers:	2	Adtl Printers:	1	Adtl Printers:	1
Help Desk:	8 x 5	Adtl Laptops:	20	Adtl Laptops:	2	Adtl Laptops:	2
Multi-User?	Yes	Rug'edzd Laptops:	0	Rug'edzd Laptops:	0	Rug'edzd Laptops:	0
Field Reporting?	Yes	Hardware:	$69,129	Hardware:	$13,534	Hardware:	$13,534
Sworn Officers:	100	Software:	$32,266	Software:	$32,266	Software:	$162,236
Remote Sites:	0	Training:	$4,350	Training:	$4,350	Training:	$4,350
Incidents per Month:	1,500	Installation:	$9,373	Installation:	$6,243	Installation:	$6,243
Concurrent Mobile	20	Conversion:	$10,609	Conversion:	$10,609	Conversion:	$10,609
Users:		**Total:**	**$125,726**	**Total:**	**$67,002**	**Total:**	**$196,972**
		O&M	**$11,451**	**O&M:**	**$5,892**	**O&M:**	**$25,387**

Size		**No RMS**		**Non-RMS**		**BR RMS**	
LARGE		Design Solution:	COTS	Design Solution:	COTS	Design Solution:	COTS
Wide Area Network		Substations Requiring		Substations Requiring		Substations Requiring	
		Adtl Bandwidth:	10	Additional Bandwidth:	5	Additional Bandwidth:	5
Help Desk:	8 x 5	Adtl Workstations:	88	Adtl Workstations:	9	Adtl Workstations:	9
Multi-User?	Yes	Adtl Printers:	12	Adtl Printers:	4	Adtl Printers:	4
Field Reporting?	Yes	Adtl Laptops:	100	Adtl Laptops:	0	Adtl Laptops:	0
Sworn Officers:	1,000	Rug'edzd Laptops:	0	Rug'edzd Laptops:	10	Rug'edzd Laptops:	10
Remote Sites:	10	Hardware:	$417,677	Hardware:	$73,926	Hardware:	$73,926
Incidents per Month:	18,300	Software:	$120,412	Software:	$120,412	Software:	$120,412
Concurrent Mobile	10	Training:	$6,960	Training:	$6,690	Training:	$6,690
Users:		Installation:	$60,900	Installation:	$25,392	Installation:	$25,392
		Conversion:	$15,914	Conversion:	$15,914	Conversion:	$15,914
		Total:	**$621,863**	**Total:**	**$242,604**	**Total:**	**$242,604**
		O&M:	**$128,194**	**O&M**	**$63,148**	**O&M:**	**$63,148**
LARGE		Design Solution:	CUST	Design Solution:	CUST	Design Solution:	CUST
Wide Area Network		Substations Requiring		Substations Requiring		Substations Requiring	
		Adtl Bandwidth:	10	Adtl Bandwidth:	5	Adtl Bandwidth:	5
Help Desk:	8 x 5	Adtl Workstations:	88	Adtl Workstations:	9	Adtl Workstations:	9
Multi-User?	Yes	Adtl Printers:	12	Adtl Printers:	4	Adtl Printers:	4
Field Reporting?	Yes	Adtl Laptops:	100	Adtl Laptops:	0	Adtl Laptops:	0
Sworn Officers:	1,000	Rug'edzd Laptops:	0	Rug'edzd Laptops:	10	Rug'edzd Laptops:	10
Remote Sites:	10	Hardware:	$417,677	Hardware:	$73,296	Hardware:	$73,926
Incidents per Month:	18,300	Software:	$2,138,134	Software:	$949,935	Software:	$207,305
Concurrent Mobile	100	Training:	6,960	Training:	$6,690	Training:	$6.96
Users:		Installation:	$60,900	Installation:	$25,392	Installation:	$25,392
		Conversion:	$15,914	Conversion:	$15,914	Conversion:	$15,914
		Total:	**$2,639,593**	**Total:**	**$1,072,126**	**Total:**	**$329,496**
		O&M:	**$430,853**	**O&M**	**$187,576**	**O&M:**	**$76,182**

3.2 Additional Cost Analysis Considerations

As an agency examines potential costs of a new RMS, there are additional acquisition considerations that should be taken into account. This section addresses three of those considerations—purchase versus lease, use of existing contracts as purchase vehicles, and total cost of ownership for the RMS.

3.2.1 Purchase versus Lease

The cost model assumes purchases of all COTS hardware and software is followed by contractor maintenance. Savings may be achieved for hardware and systems software through bulk buy, bulk lease, or bulk maintenance agreements available in an agency's city, county, or state. For comparison purposes, it should be noted that Gartner Group recommends personal computer replacement in a normal office setting every 5 years. A machine used by 24-hour shifts or in a patrol car would have a shorter "shelf life." The primary useful life of a standard notebook/laptop is 30 to 36 months (Gartner Group presentation "PDAs, Smart-phones and Notebook Computers," March 2000). The historic equipment replacement cycle in the agency should be considered in calculation of system's life cycle costs and for cost analysis of a lease versus buy decision. All estimates should include the cost of spare units. Calculation of the number of spare units needed is based on average historic downtime and the mean time between failure (MTBF) rate.

Purchase versus lease of equipment is not always just a cost decision. Purchase of the device eliminates any questions about who owns the data on the device, reduces machine switching by the leasor or maintenance contractor (a security and asset management factor), and simplifies asset tagging of purchased equipment for agency inventory control.

3.2.2 Use of Existing Contracts

The agency should research its existing equipment acquisition and maintenance contracts and also those that the state may have on file. Agencies should analyze whether or not a current contract for maintenance can be modified to add the NIBRS-RMS units. This approach may be easier to fund and/or cheaper than negotiating a separate agreement for a NIBRS-RMS. Likewise, large agencies may have ongoing software contracting agreements that may be used. In some circumstances, an agency may be able to purchase the system from the GSA schedule or similar contracts within the agency's state. The contracting office should be able to help in searching for these contracts.

3.2.3 Life Cycle Cost and Total Cost of Ownership Issues

The strategic plan developed by the NIBRS-RMS project team should consider the life cycle costs of procuring and maintaining the system as well as the cost and benefits across the entire agency, not just IT. The emphasis should be on the most cost-effective way for the agency to obtain, use, and maintain an up-to-date NIBRS-RMS. The current IT staffing level, skill levels, conflicting priorities, and internal learning curve are considerations. The functional requirements of the entire proposed system should be analyzed to identify which functions in-house staff, COTS products, or contractors can best supply.

The analysis of current and new business processes helps to identify the cost impacts of the new system in non-IT departments. In particular, additional clerical staff needed for data entry and reports, the number of people by job category to be trained in the use of the new system, and the impact of training time on other job functions should be carefully reviewed and estimated. If an agency is going to "train the trainers," they will need to consider the following questions. How many trainers will be needed? What travel expenses will be needed to train the trainers or users? How does training time vary for different categories of users? Which organization does follow-up training? How does the use of the new system impact the job skills required of current personnel and new hires? What is the impact of the new system on the computer help desk?

Agencies should consider that organizations must base their decisions on development and maintenance expenses, not capital expenditures, as the latter represent only 20% of the overall cost of the application ownership (Joseph Feiman, Gartner Group "Applications Development by the Numbers: Justifying Technology Choices," March 2000).

3.3 Federal Funding Sources

All funding sources should be explored by the agency. For example, many states have arrangements by which they help cover the cost of a new NIBRS-compliant RMS.

The major out-of-state funding source is the federal government. Within the federal government, there are several potential sources of funds. The primary potential sources of federal funding for NIBRS projects are described below.

3.3.1 OJP CITA

Office of Justice Programs (OJP) Crime Identification Technology Act (CITA) See Website at http://www.ojp.usdoj.gov/ocpa/ataglance/technology.htm. Information on future CITA funding is not available at this time. For information on the most recent CITA solicitation, which closed August 31, 2000, see:

http://www.ojp.usdoj.gov/bjs/abstract/nibrsip.htm (excerpted below).

National Incident-Based Reporting System Implementation Program Solicitation

- AGENCY: Office of Justice Programs, Bureau of Justice Statistics.
- ACTION: Solicitation for award of cooperative agreements.
- SUMMARY: The purpose of this notice is to announce a public solicitation to make awards to states to provide funding to jurisdictions for implementing the National Incident-Based Reporting System.

CITA - NATIONAL INCIDENT-BASED REPORTING SYSTEM
Pub. L. 105-251, 42 U.S.C. § 14601

FUNDING: FY2000 Funding: $10 Million
FY2001 Funding: $7.1 Million
FY2002 and 2003 Funding has not yet been allocated

GRANT PROGRAM INFORMATION: The NIBRS program moves beyond aggregate statistics and raw counts of crimes and arrests that comprise Summary UCR, to include individual records for each reported crime incident and its associated arrest. Incident-based reporting allows state and local jurisdictions to capture detailed offense, offender, victim, property, and arrest data. In addition to changing the fundamental reporting structure underlying crime and arrest information, NIBRS collects offense and arrest data on 22 crime categories, spanning 46 offenses. NIBRS funding comes from a portion of the $35 million discretionary funds under the Crime Identification Technology Act allocation.

ELIGIBILITY: The NIBRS awards are made to states applying on behalf of one or more cities or counties in the state, regardless of whether the state maintains a UCR program. Within the state, requests may be made on behalf of one or more jurisdictions or a collaboration of jurisdictions. In addition, a state can apply for funding to be used at the state level, provided that the state also applies for funds on behalf of a city or county jurisdiction. BJS will select the jurisdictions to be funded. The program will be competitive between and within states and requests for state funding will compete against requests for funding for cities and counties. Because of limited funding, not every state will receive an award, and the grants may not cover the entire costs of the conversion to NIBRS.

All awards will be made to the state that will transfer funds to the selected jurisdictions as appropriate. The proposal must present a separate budget for each jurisdiction or collaboration and describe procedures for transfer of funds.

Applications requesting funds for more than one jurisdiction must include an approval signature from the appropriate official in each jurisdiction proposed for funding.

States interested in obtaining funding for NIBRS implementation under this solicitation, should contact either their state ASUCRP representative on their Website - http://www.asucrp.org/ or the state agency designated by the Governor to apply for federal NIBRS funds. Applications should include a cover memo from the ASUCRP member. If the applicant agency differs from the ASUCRP member's agency, the selection of the applicant agency should be explained.

CITA requires that states receiving funds appropriated under the Act certify support for the FBI's National Instant Criminal Background Check System (NICS) and that a statewide strategy for information sharing is in effect or will be initiated. CITA also requires that fund recipients provide a 10% "match" of the total project cost.

3.3.2 NIJ VAWFV

National Institute of Justice (NIJ) Violence against Women and Family Violence (VAWFV). See Website at http://www.ojp.usdoj.gov/nij/funding.htm.

See NIBRS project at http://www.ojp.usdoj.gov/nij/vawprog/grnt_2000_03.html.

3.3.3 COPS MORE

Community Oriented Policing Services, Making Officer Redeployment Effective (COPS MORE)
See Website at http://www.cops.usdjo/gov/ (excerpted below).

SUMMARY: Up to $81 million in grant funding is available to U.S. law enforcement agencies for the purchase of information technology systems during federal fiscal year 2001 (ending on September 30, 2001).

COPS MORE 2001 provides funding for only the following general categories of technology:

- Mobile computing systems.
- Personal computer systems.
- Computer-aided dispatch systems.
- Records management systems.
- Crime analysis hardware/software.
- Automated booking systems.
- Automated fingerprint identification systems.
- Video arraignment systems.

Note: Funding for civilian personnel are not available under COPS MORE 2001.

3.3.4 Others

Many major grant programs administered through OJP authorize equipment purchases, generally including hardware and software. Such programs include the Byrne Formula Grant Program, the Byrne Discretionary Grant Program, the National Criminal History Improvement Program, and the State Identification Systems Grant Program. For information about the NIBRS grants or other funding through OJP or one of its five bureaus, agencies should visit the OJP Internet site at http://www.ojp.usdoj.gov (click on "Publications" and then "Guidelines, Solicitations, and Application Kits"). The National Criminal Justice Reference Service (NCJRS), clearinghouse for the Bureau of Justice Assistance (BJA) provides additional information regarding funding opportunities on the Internet at http://www.ncjrs.org (click on "Law Enforcement," "Topics," then "Justice Grants").

3.4 Lessons Learned from NIBRS User and Vendor Communities

The following list contains "lessons learned" and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Agencies should refer to this list for practical advice that can be used in conjunction with the items specified in this section of the handbook. Comments from NIBRS-RMS vendors have been included where appropriate. The comments in this list do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor community.

Lessons Learned from Agencies:

- Combine with other agencies in county or region for a NIBRS-RMS together.
- Get twice as much money as you think you need . . . it "snowballs very quickly."
- Apply for many grants.
- State programs should try to do their best to get money/funding to actually help their agencies implement NIBRS-RMS.
- Many times, grants are not enough. Pursue capital improvement funding.
- Go after as much law enforcement grants as possible.
- Be sure that grants are for purchasing hardware, the NIBRS-RMS software, and all elements of the system. Otherwise, some things will be missing and the system (and you) could suffer.
- Convince whomever gives you funding that it is for "continuing operational expense" not just for a "capital expense" because you will need the funding for more than just to get started.

Lessons Learned from States:

- Combine with other agencies in county or region to obtain a NIBRS-RMS together.
- State programs should try to do their best to get money/funding to actually help their agencies implement NIBRS-RMS.
- Go after as much law enforcement grants as possible.
- Be sure that grants are for purchasing hardware, the NIBRS-RMS software, and all elements of the system; otherwise, some things will be missing and the system (and you) will suffer.
- The state provides support and encouragement to agencies to convert to NIBRS with matching funding provided to local agencies.

4 SELECT RMS VENDOR

Once an agency has defined its RMS requirements (see section 2) and obtained funding, it can proceed to acquire the RMS. This section assumes that an agency will competitively acquire a COTS RMS package from a qualified vendor. The steps to be followed are described in subsections below:

- Define the Procurement Process.
- Define Acquisition Strategy.
- Develop RFP and Schedule.
- Conduct Source Selection.

4.1 Define the Procurement Process

An agency's first step must be to contact the appropriate contracting office. This should be done at the very beginning of the project because the office can contribute advice and guidelines for many of the system-definition steps. The contracting office can also provide specific acquisition procedures and regulations and may require that it manage the acquisition. If the contracting office does not manage the acquisition, someone from the office should be a key part of the acquisition team.

The contracting office will determine what steps should be followed. These may vary somewhat from the steps described below. The advice of the contracting office ensures that an agency's acquisition meets all applicable local, state and federal regulations and policies. For example, there may be regulations and policies for the project funding, fiscal yearn budgeting, contract management, and payments/invoices. The earlier an agency obtains information on applicable procedures and policies the easier it will be for the agency to proceed.

Regulations and policies can have a major impact on the source selection process. For example, an agency's city or county may require that a certain percent of the total contract value go to local minority or women-owned business enterprises. This can result in a single acquisition being split into two or more parts—software package, hardware and system software, and system engineering/support contractor (to help with file conversions, etc.).

Alternatively, some systems or components can be acquired off of the General Services Administration (GSA) schedule. The procuring agency should still evaluate and compare systems and capabilities, but negotiations and contract award time may be greatly reduced with a GSA schedule purchase. Savings can also be achieved by using blanket purchase agreements and government-wide agency contract (GWAC) programs procuring IT systems, maintenance, Help Desk services, and systems engineering.

Using a GWAC procurement vehicle can help the agency to achieve lower prices, as well as provide procurement management assistance, provide a competitive procurement among the corporations that were selected by the host agency to be involved in the GWAC, and expedite the procurement process. The GWAC host agency charges a management fee. Although state and local agencies cannot use the federal government GWACs, some states are establishing GWAC-like procurement arrangements for state agency procurements.

The contracting office will probably want the system competitively procured, as opposed to "sole source" procurement where the agency chooses the RMS vendor without competition. The goal of competitive procurement is to obtain the system that best meets an agency's needs for the best value, not necessarily the lowest cost. The contracting office emphasizes fair and open competition so that no single vendor has an undue edge in the competition and legal challenges from losing vendors can be avoided.

4.2 Define Acquisition Strategy

During system definition, the project team defines the system's functional requirements and design. In source selection, the team must give thought to how the agency will acquire the total system. For larger agencies, the team should prepare an acquisition strategy so that all factors are considered and the plan is well defined. There are several factors that must be taken into consideration in the acquisition strategy:

- **Phased Implementation.** Is the system to be implemented in phases? If so, should the agency acquire all parts of the system initially or wait and acquire components pertaining to later phases under a separate acquisition? If the agency chooses different vendors for different components, what will be the impact on system operation? Who will integrate the components? Is system acceptance the last phase or is an O&M phase included in the acquisition contract?
- **Separate Hardware.** Does the agency plan to acquire the hardware (and its corresponding system software) separately from the COTS RMS package? If an agency plans to do this, it should have the configuration defined by the RMS vendor. This could cause timing problems since the hardware configuration cannot be purchased until the RMS vendor is selected. Is an agency or a contractor responsible for systems integration?
- **Other Systems.** Are there additional systems that must be acquired concurrently with the RMS? For example, an agency could decide to acquire MDCs as part of the RMS implementation (implementing the major subsystems in phases would be advisable in this case).
- **System Engineering/Support Contractor.** Does an agency require the support of either a system engineering company to help fit the pieces together into an integrated system or a support contractor to help with one-time chores such as file conversion and training?

If an agency plans to have more than one acquisition, it must prepare separate procurement packages. The agency may also refine separate evaluation teams for each acquisition.

For the small agency, acquisition should be fairly straightforward. It is unlikely that any of the complicating factors discussed in section 5.2 will impact a smaller agency.

4.3 Develop RFP and Schedule

The agency should assemble a package of materials that completely describes what the agency wants to buy and how it plans to do so. This package is called a request for proposal (RFP). An agency's contracting office will be able to provide guidance and/or samples of what is needed in its RFP. Table 4.1 Uniform Contract Format from the Federal Acquisition Regulation (FAR) can be used as a checklist for the contents of an agency RFP. These regulations provide helpful guidelines, standardized contract clauses, and definitions of terms.

For further information agencies should reference the website http://www.arnet.gov.

Table 4.1 Uniform Contract Format
Source: Federal Acquisition Regulation section 15.204-1

Section	**Title**
Part I The Schedule	
A	Solicitation/Contract Form
B	Supplies/Services and Prices/Costs
C	Description/Specifications/ Statement of Work
D	Packaging and Labeling
E	Inspection and Acceptance
F	Delivery and Performance
G	Contract Administration Data
H	Special Contract Requirements
Part II Contract Clauses	
I	Contract Clauses required by law
Part III List of Documents, Exhibits, and Other Attachments	
J	List of Attachments
Part IV Representations and Instructions	
K	Solicitation Provisions (required representations, certifications, or submission of other information by offers)
L	Instructions, Conditions, or Notices to offers or respondents
M	Evaluation Factors for Award

In general, to ensure fair competition, the procurement process must have these key elements, which may be documented separately or together:

- **System Specification.** Well-written description of the system the agency wants to buy (see section 2).
- **Statement of Work.** Clear definition of exactly what the agency expects the vendor to do.
- **Instructions to Bidders.** Clear instructions on what the vendor must do to submit a proposal.
- **Evaluation Plan.** Fair evaluation process defined in advance.

After the agency places advertisements in appropriate publications (as defined by the contracting office) and state/local government web sites, interested vendors will respond by requesting copies of the RFP. If the contracting office chooses to have a bidder's conference, vendors are able to attend and ask questions about the procurement. All attendees must register in a logbook when they arrive. To ensure equal access to all vendor information, notes are taken at the meeting and a copy of all vendor questions and agency responses is furnished to all attendees. Vendors may be able to send additional questions to the contracting office prior to a specified date and all questions and answers are distributed to all bidders. To be considered for evaluation, the vendor's proposal(s) must be in the contracting office before the closing date and time specified in the RFP to be considered in the evaluation. For a large procurement, a vendor may be required to submit to contracting office a technical proposal, a cost proposal including basis of estimate, a management proposal including references and schedule, and appendices.

4.3.1 Statement of Work

The statement of work (SOW) must have specific categories of tasks that clearly define the work that the agency expects the vendor to perform. If mandatory work is not listed in the SOW and the contractor does not include it in the price, there is no obligation to perform the work. Obviously, careful attention must be paid to this area.

Some agencies have assumed that once a vendor has sold the agency its software package, the vendor will be there at all times to help solve problems. Many of these problems originate with the agency, not the vendor, for example converting a file or adding a new software module. This kind of support may be possible, *but* it must be defined in the statement of work and included in the budget or it will not be covered in the contract.

Some example task *categories* for competitive procurement of a COTS RMS are:

- **General Management and Administration.** This task category addresses the kind of project management the agency expects from the vendor. It includes how the agency's project will be managed by the

vendor, development of a project plan, quality assurance and periodic progress reporting.

- **COTS Software.** This task category requires the vendor to deliver software that meets the RMS specifications defined in the RFP. It also includes the expected delivery schedule. If the project is to be implemented in phases, then specific functions and capabilities must be defined in the RMS specification. Again, delivery dates must be included for each phase.
- **System Verification.** This category specifies all RMS tests and demonstrations that the agency wants performed, along with a timetable. It also designates responsibilities (for example, who is responsible for test scripts or test data).
- **Documentation.** This category requires the vendor to provide adequate documentation of its product and its operation, system administration, and security administration. It could also include early delivery of the database structure documentation so that an agency's IT staff can have an understanding of the system's operation. Some agencies require the source code to be put into escrow. In the event that the vendor discontinues support of the product, the agency will be able to use the code for continued system upgrade and maintenance either by in-house staff or by a contractor.
- **Training.** This category requires the vendor to provide a training plan for the agency. It includes training in the use, administration, and security of the system. Vendors often include "train-the-trainer" costs in their product pricing.
- **Transition and Data Conversion.** This category defines vendor assistance in areas such as file conversion, code entry and other transition actions. A certain number of hours may already be included in the vendor's product pricing. Since it is difficult to define this work precisely during source selection, the agency can ask the vendor to quote hourly costs for different types of support including clerical and administrative and/or a technical advisor to help in specific activities.
- **System Engineering.** This category requires the vendor to provide engineering assistance in technical areas such as development of ICDs for interfaces with other agencies or potential (unspecified) customization of the software. Again, the vendor may include some support in this area as part of its product price. Since it is difficult to define this work precisely during source selection, the agency can ask the vendor to quote hourly costs for engineering support.
- **Maintenance and Support.** This category requires the vendor to provide on-going support for the RMS software. This includes maintenance support to correct software errors and upgrades to the product. Some support is already included in the vendor's product price. An agency may want to extend that support in terms of months of coverage and hours per day. For example, a large agency with a complex system that has

extensive on-line interactions may want to have a RMS engineer on-site for certain periods of time.

- **Hardware Configuration.** This category requires the vendor to provide hardware (and its corresponding system software) sufficient to meet the performance requirements defined in the RMS specification. If the RMS vendor also provides the processor configuration, then the requirements for this would be covered in this category. If the agency acquires the processor configuration separately, then it should ask the RMS vendor to deliver specifications for the processor configuration that would allow the performance requirements to be met.
- **Deliverables.** This category summarizes the vendor obligations, which are often termed "Contract Deliverable Line Items" or deliverables. A table listing each deliverable and its due date should be included in the statement of work.

4.3.2 Instructions to Bidders

Prospective bidders are given formal instructions on how to submit their proposal. These instructions are usually prepared by the contracting office and should address where the proposal is to be delivered, by what time it must arrive, any size restrictions, and the overall format of the proposal. Many agencies recommend that these instructions require the vendor to submit a list of past clients (law enforcement agencies) who have purchased the same or similar systems and services from the vendor and/or subcontractors. Prospective bidders should also address issues such as subcontracting plans, restricted rights to software, source code escrow, and instructions on the format of the response. Using a common format simplifies the proposal evaluation effort.

Typically the cost portion of the proposal is submitted under separate cover so that technical evaluation can proceed separate from cost evaluation. A precise format of costs should be given to the vendors so that cost evaluation is simplified. Finally, the instructions should ask for the vendor's corporate resources and qualifications.

4.3.3 Evaluation Plan

The evaluation plan describes how the agency and its contracting office plan to evaluate the proposals the agency receives from vendors in response to the RFP. It includes factors to be used in proposal evaluation and their relative importance. Examples are given in Table 4.2. An agency should consider which factors are most important. For example, is the agency willing to pay a little extra for the assurance of on-time delivery?

In the course of evaluation, the agency should research the past performance of the bidder and subcontractors. It is recommended that the technical evaluation

team be responsible for this factor. (See section 4.4.) Agencies should keep in mind that the agency cannot *require* that a particular individual (i.e., a specific program manager or technician) work on the contract after award.

Table 4.2 Example Evaluation Factors

Evaluation Factor	Description	Weight
Cost	Evaluate costs of qualified proposals.*	25
Schedule	Evaluation realism of the schedule of proposals.	15
Technical	Evaluate the extent to which qualified proposals meet *desirable* requirements.	30
Corporate Resources and Qualifications	Evaluate the following factors: Project Manager—relative experience Corporate Experiencer—relative experience Corporate Past Performance—relative success as verified through conversations with past clients.	20
Demonstration	Evaluate success of each vendor's product demonstration.	5
Risk	Evaluate risk of proposals, considering likelihood of on-time delivery, newness of the product, etc.	5
* A qualified proposal is that which meets all *mandatory* requirements.		

4.4 Conduct Source Selection

The source selection process begins at the closing date for proposal submission. The proposal evaluation process may be managed by the contracting office and must be structured and closely observed to ensure objectivity. The contracting office must specify early in the procurement process whether there can be preliminary proposals followed by written evaluations of discrepancies, oral meetings with each bidder, and a best and final offer, or if the first proposal submitted is considered to be best and final.

A technical evaluation team, consisting of a few key project people from the agency, will evaluate and score each proposal on its own merits. The agency or contracting office must reject any proposal not meeting the *mandatory* requirements. Part of the technical evaluation may be an assessment of product demonstrations made by qualifying vendors. It is recommended that the technical evaluation team verify the vendor's past performance, particularly the system's NIBRS capabilities, by contacting past clients. Parallel to this technical evaluation, the contracting office will evaluate the cost proposals.

The results of the technical evaluation are forwarded to an evaluation panel, which may consist of the project manager, contract manager, and other key

agency managers. Based on the evaluations, the panel will rank the proposals and present the results to the source selection officer, who will be a senior manager. If the source selection manager concurs with the analyses, the winner is announced. This culminates in the signing of the contract. Bidders who did not win are usually offered the opportunity to be debriefed in individual meetings with the selection officer and contract staff.

4.5 Sample RFPs

Actual RFPs and requests for information (RFIs) used by agencies to procure RMSs are available at http://www.it.search.org/default.asp, the IT Acquisition Database maintained by SEARCH for BJS. To the left of the screen is the "Find a Document" feature. Select "Criteria Query." On the query screen, click on the checkboxes for "Records Management System" and "RFP" and submit the query. A list of the RFPs available from the database is displayed.

4.6 Procurement Lessons Learned

The following list contains "lessons learned" and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Agencies should reference this list for practical advice that can be used in conjunction with the items specified in this section of the handbook. Comments from NIBRS-RMS vendors have been included where appropriate. The comments in this list do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor community.

Lessons Learned from Agencies:

- Make RFP very specific in what you want.
- Vendor demo is not enough. Must conduct site visits and contact current users of vendor's products.
- Just because vendor says 'NIBRS-compliant' means nothing. Make absolutely sure that vendor's product is NIBRS-compliant AND that it is capable of meeting all state requirements for certification in the particular state.
- COTS system that we purchased met NIBRS compliance but had to be customized to meet state needs, which are more extensive than NIBRS.
- Look for NIBRS-compliant RMS, but use caution—some vendors say they are NIBRS-compliant, but are not.
- Check to see if the new RMS accepts mug shots so that they can become part of the RMS records.
- Do hands-on evaluation of vendor products—perhaps through demonstration—BEFORE contract.
- You want to work with the vendor's actual developers, not just the vendor's managers.

- Look closely at the need for custom programming; will it be covered by the maintenance agreement?
- RMS software was not NIBRS-compliant, but the software company made changes for nothing so that their software would be certified for NIBRS reporting.

Lessons Learned from States:

- Identify your own needs first.
- Don't sign off on anything with the vendor until you're fully satisfied with the product.
- Talk to other users of vendor products.
- Check out vendors with other users.
- Identify milestones in the contract.
- Put opt-outs in contract (for example, a stop work after the requirements document in case you don't like it, or after system design, etc)… penalty clauses.
- We sent out RFQ to 7 vendors, got 5 responses. We shared our Vision with the vendors to see if they wanted to "join up."
- Don't ever purchase any vendor products that are not certified/approved/acknowledged by your state program.
- Don't invest a lot of money in vendors that have no NIBRS experience and are not confirmed to be NIBRS-compliant.
- Actually test the vendor's system before taking any further steps.
- Check around with other agencies to get opinions and experiences with vendor's products.
- Vendors get certified in the state when they successfully implement a NIBRS-compliant system in the state.
- Most agency complaints are about vendors that did not perform—lots of promises, but when problems occur, the vendor often does not support the agency.
- Formed a state-level committee to discuss how to address non-performing vendors.

Vendor Comment:

- Make sure the state trains the agencies on their reporting demands and that these demands are included in the RMS specifications so that the new RMS software does not get blamed when the reporting is wrong.

CHECK LIST FOR RMS VENDOR SELECTION

- **Define Procurement Process—**Work with contracting office to define overall approach for buying the RMS.

- **Define Acquisition Strategy:**
  - **Implement in Phases?** Affects how procurement is done.
  - **Hardware Separate from RMS Software?** Can affect schedule and result in two procurements rather than one.
  - **Other Systems Simultaneously?** Will other systems, such as local area network or MDCs be purchased at the same time?
  - **Support Contractors?** If an agency needs support contractors for implementation, they must be procured prior to implementation**.**

- **Develop RFP and Schedule**:
  - **System Specification—**See section 2.
  - **Statement of Work—**Defines what the vendor is to do.
  - **Evaluation Plan—**Defines how proposals will be evaluated.
  - **Instructions to Bidders—**Instructions to vendors on how to submit a proposal.

- **Conduct Source Selection and Negotiations:**
  - **Technical Evaluation Team**
  - **Demonstrations**
  - **Cost Evaluation Team**
  - **Best and Final Offers**
  - **Source Selection Panel**
  - **Source Selection Authority**
  - **Negotiations**

- **Notes and Comments:**

5 PLAN AND MANAGE IMPLEMENTATION

This section describes the planning and management responsibilities that an agency will have once the system vendor is selected or once the system design is chosen for those agencies developing their own system. Section 6 describes the activities specific to RMS system installation, and section 7 addresses the steps to be taken to prepare the agency's staff and business processes for NIBRS reporting and for using the new RMS.

The activities described are more appropriate for those agencies implementing complex systems, usually larger agencies. Small agencies should address most of these areas, but at a simplified level. For each area, the potential activities for a small agency are described.

Outsourcing. Some government agencies are considering, or in some cases already have, outsourced their information processing operations. Outsourcing means that an agency signs a contract with another agency or a commercial firm to operate the RMS and assume responsibility for the NIBRS reporting. Some law enforcement agencies feel that the information is too confidential and too important to entrust to any entity other than their own. On the other hand, some law enforcement agencies have outsourced at least part of their RMS and/or crime-reporting functions. The activities in this section assume that an agency is planning to operate the RMS rather than outsource its operation. *Even if an agency chooses to outsource RMS operations, a project manager and team thoroughly familiar with the RMS, NIBRS, and system operations will still be needed.*

System integration contractor. Some agencies may opt to hire a single contractor to perform their system definition, hardware and software integration, installation, and operation. For larger agencies with complex systems, working with a single contractor provides the distinct benefit of obtaining help and answers from one source. The system integration cost, however, may be considered high by the agency. If an agency is concerned about being able to attract competent personnel to perform critical planning, implementation, and operations, the agency may want to hire an integration specialist. *The agency should make sure that the contract clearly defines what the integration specialist will and will not do. Again, a project manager and team thoroughly familiar with the RMS, NIBRS, and the system operation are still needed.*

Implementation planning and management involves the following steps, each of which is described in the sections that follow:

- Establish Implementation team.
- Prepare and Maintain Implementation Plan.
- Prepare and Maintain Risk Management Plan.
- Prepare O&M Budget.

- Hold Periodic Implementation team Meetings.
- Plan and Manage System Security.
- Develop Interface Control Documents.
- Convert Files.
- Develop Test, and Acceptance Plan.
- Develop Training Plan.
- Monitor Vendor Performance.

5.1 Establish Implementation Team

The project manager must assemble the implementation team. This team may include some of the same personnel that were part of the RMS definition team, but there will be differences. While the selection team includes managers that understand the agency's needs, the implementation team will consist of hands-on people that plan, perform physical plant upgrades, monitor vendors, convert files, test systems, prepare training, etc.

The number of people on the implementation team and the percentage of their time required depend on the size of the project and the project manager's experience. In larger agencies, the project manager needs a staff of full-time people; in medium size agencies, the staff may be smaller or part-time. Teams that are most effective have staff drawn from the departments most affected by the move to NIBRS and the new RMS.

The implementation team should include one or more representatives from the information systems operations staff, even if operations services are outsourced. If an agency currently operates other information systems, someone familiar with those operations must understand the RMS and determine how it will affect the operations center. For agencies where the RMS is the first major information system, the agency must decide how to staff the RMS operation. The agency must have at least one staff member who understands the fundamental operation of the system, and can diagnose problems, install new software releases, maintain documentation, ensure system integrity and security, and help users with problems. This could be someone the agency hires, or it could be a contractor. Staff will be needed to deal with supplies (for example, printer ink and paper), telephone line connections, periodic file backup, archives, logs, etc. The staff assigned to perform these activities will require some level of technical training, depending on the software and hardware technologies used and the experience and training of assigned individuals.

The RMS working groups must remain intact since they will provide a vital liaison between the implementation team and the agency's various departments. They should have people with knowledge of all of the business areas that will be affected by the new RMS. The working groups must operate as teams, so management must be prepared to allocate a portion of their working hours to the working groups. The groups must be kept small enough to be effective, so there

may be multiple groups with responsibilities divided among them. As discussed in section 2.1, representation needed in the working groups includes:

- A command staff member.
- Patrol officers.
- Case investigators.
- Records personnel.
- Prosecuting attorneys.
- Courts.
- Crime analysts.
- Special areas (depending on the scope of the RMS being procured).
- Business Process staff.
- Technical staff.

Table 5.1 illustrates the kinds of resources that may need to be allocated to the implementation team for three different size agencies.

Table 5.1 Implementation Team Staffing for Different Size Agencies

Project Staff Type	Number Of Sworn Officers		
	10	100	1,000
Project Manager	1 part or full time	1 full time manager	1 full time manager plus assistant managers
Project Staff	Some outside aid	Part-time representatives of some departments	Full and part-time representatives of all major departments

5.2 Prepare and Maintain Implementation Plan

Implementation of an information system requires a large number of intricately inter-related activities that must all come together if the project is to be successful. A detailed RMS implementation plan must be developed and religiously maintained. This plan is the basis for determining what is to be done, when, and by whom. It is also the primary focus of the implementation team meetings.

For a small agency, the implementation plan is still very important. It will describe everything that must be done by the agency. The RMS vendor, other agencies, or an outside contractor can help put this together.

The implementation plan should be developed in cooperation with the RMS vendor, who should contribute to the descriptions of the implementation actions that need to be performed. Personal computer project management tools, such as Microsoft Project™, can be used to develop and maintain the schedule and resource parts of the implementation plan. Figure 5.2 is an implementation flowchart for the tasks described in this handbook.

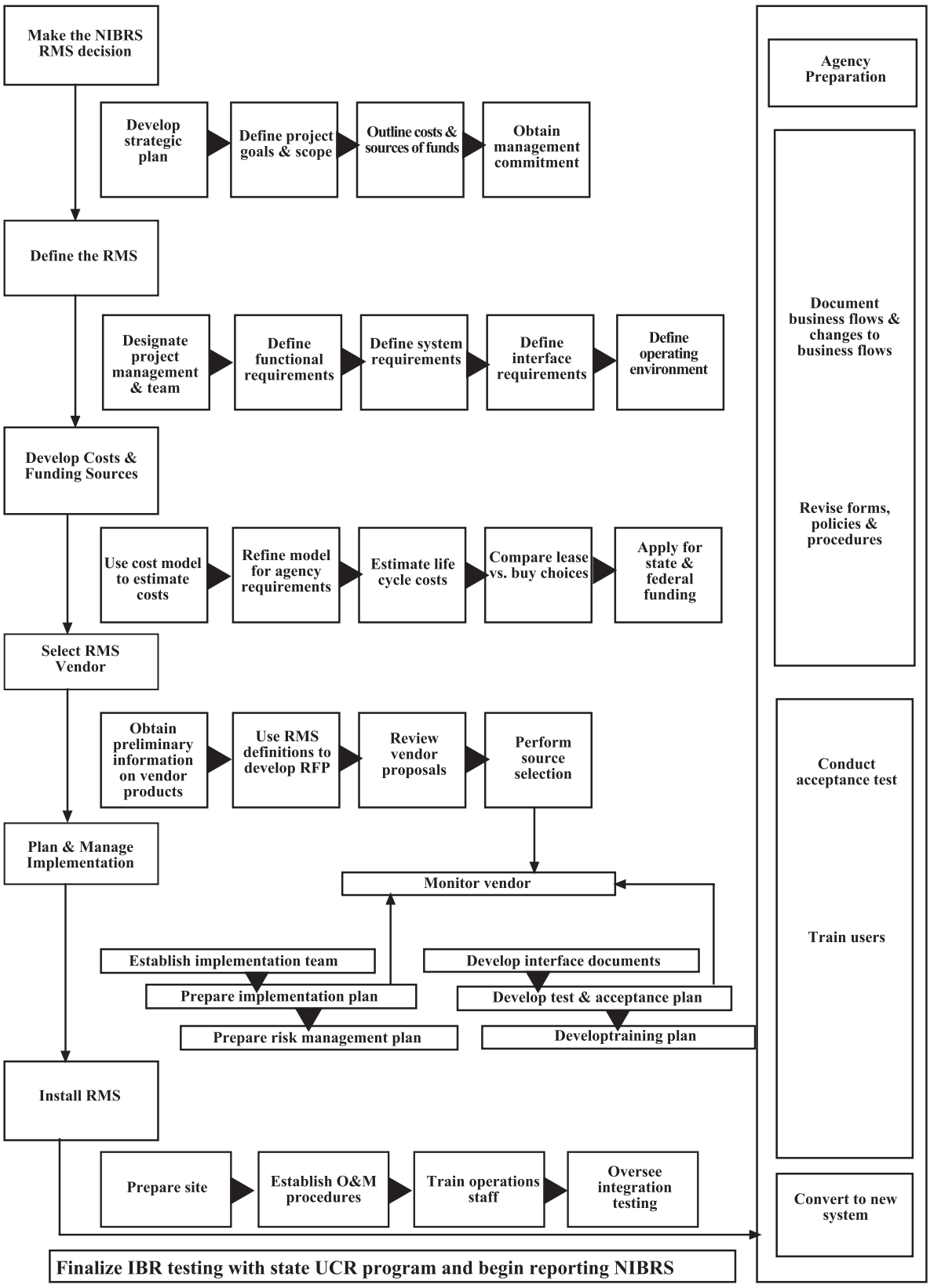


Figure 5.2 Implementation Flowchart

5.3 Prepare and Maintain Risk Management Plan

The risk management plan is developed and maintained along with the implementation plan. It identifies the risks, and their severity, associated with each step of implementation. It is updated at each implementation team meeting. As risks are reduced or eliminated, they are removed from the list of risks. As new risks arise, or old risks increase in severity, a plan for mitigating each risk is developed. For example, if the new processor cannot be installed until the electric service is upgraded, and the electrical workers union goes on strike, then the risk of missing the installation deadline would increase; someone would be assigned to look at alternative approaches to reduce the risk.

For a small agency, a separate risk management plan may not be necessary; however, the project manager must still identify risks and act to mitigate them—with or without a formal plan.

5.4 Prepare O&M Budget

The project manager is responsible for developing an O&M budget for the RMS and NIBRS reporting operations. This can be developed once the vendor is selected and the O&M approaches are known.

5.5 Hold Periodic Implementation Team Meetings

Periodically (weekly for larger projects), the project manager must meet with the key implementation team members to assess the progress. These meetings are very important since they allow individuals on the implementation team to interact and resolve problems or approaches among the various activities. In these meetings, there should be rigorous assessments to determine if the implementation is on schedule, if the agency's requirements are being met, and what new actions must be taken.

For a small agency, the project manager should have periodic meetings with the RMS vendor and with other key staff that will be affected by the system to make sure that the implementation is progressing as planned.

Although the implementation team are the primary attendees, working group members and other agency staff may be included if they have important information or are performing important RMS-related activities.

5.6 Plan and Manage System Security

Because sensitive information will be on the RMS, protection from unauthorized access, disclosure, and modification is imperative. Security and privacy are

addressed through a variety of physical and computer security services. The purpose of these services is to ensure:

- *Confidentiality of all data*—who is authorized to see the data?
- *Integrity of all data*—who can modify and delete data, and who audits the transaction logs?
- *Availability of the system and data*—can the data and network be accessed whenever necessary?
- *Authentication*—can you make a positive identification of the systems' users and determination of their authorities?
- *Non-repudiation*—do you have the ability to defeat claims of non-participation of a user in a transaction?

Processor and communications security. There are a variety of security approaches that can be used on the processor and communications systems to provide some level of security. The level of sophistication varies from passwords to firewalls and Public Key Infrastructure. The approach an agency uses should be chosen based on the volume of communications the processor would have with other processors. Some agencies also plan to have Internet access to the processor by law enforcement personnel or by the public to select portions of the file system (e.g., Sex Offender File). The volume of processor-Internet communications also needs to be taken into account. Talking to agencies with similar configurations and to information security consultants will help determine the best approach.

For a small agency, the RMS vendor should offer some password protection so that only those who have authority can access the system. Agencies should ensure that computer files are backed up, preferably daily; this may require the addition of a backup function to the computer system. Providing for a periodic printout of key information for use as backup in case the processor fails will supply a basic contingency plan. Finally, it is important to ensure that only authorized people are permitted physical access to the processor and the backup media and files.

System availability. Sometimes systems fail and must be recovered. Other times there can be physical, network, or software attacks (e.g., viruses) on the processor and its data files, perhaps by a disgruntled employee. It is important that agencies regularly perform periodic backups of all files and exercise file restoration procedures. In addition, agencies should consider a backup or contingency plan for the overall system processing capability. If the processor fails for any period of time, there should be a plan for emergency processing backup. With Internet connections, computer software can help protect against an Internet-based attack aimed at over-loading the processor and making it unavailable.

Physical security. An agency's operation should be in a secure area. This ensures only authorized personnel are permitted near the processing center and surrounding equipment, including communications equipment.

5.7 Develop Interface Control Documents

Interface Control Documents (ICDs) describe information exchanges between processors. Specifically, ICDs describe the information the agency wants to obtain (or send) and the procedure and format governing the exchange. Part of the ICDs is nontechnical, and other parts are technical and deal with protocol and exchange rules. ICD development requires a technical person to negotiate with other interfacing agencies and to provide comprehensive understanding of the desired data. ICDs must be maintained as systems and exchanges are modified or updated.

For a small agency, it is unlikely that automatic data exchange will be required; but if it is, an ICD for each exchange must be developed.

If the RMS is going to automatically exchange data with another processor, such as the state NCIC switch or the courts, agencies must negotiate an ICD with each entity involved. An ICD is also required if the processor is attached to a LAN. RMS vendors are usually willing to participate in ICD definition. The vendor's rates for this and all other prospective advisory services should be established during the source selection and included in the agency's contract with the vendor.

5.8 Convert Files

Prior to operation of the new RMS, the electronic RMS files must be built up from historical records. Historical records can be computerized by converting existing files and data elements into the new RMS database format. Agencies must make sure the information entered is properly coded in accordance with NIBRS and is as accurate and complete as possible.

Existing RMS. If an agency already has an RMS, then it may be possible to develop software that automatically converts old files to the new format. Generally, however, this is very difficult and only partially successful. File structures are different (e.g., the old file structure may be flat while the new RMS relies on a relational database), information fields are different (e.g., the new file has information that is not contained in the old files or vice versa), and field formats vary (e.g., number of characters used for name). The information that cannot be captured or converted automatically must be manually entered and reformatted for the new RMS, with incidents recoded according to NIBRS standards. To ensure that this is done correctly, oversight responsibility should be assigned to experienced and knowledgeable records personnel.

No existing RMS. File conversion will be from manually maintained files. To ensure that data elements are properly formatted and encoded with NIBRS incident codes, oversight responsibility should be assigned to experienced and knowledgeable records personnel.

Conversion Strategies. For either automatic or manual file conversion, an agency must look carefully at the quality of data in the current system. Are the data complete? Are they accurate? Are there duplicate records? Ideally, the file conversion effort gives the agency a chance to develop or update records management policies and "clean up" converted records so that they conform to these policies. Regardless, agencies should be aware that the entire RMS conversion effort requires commitment of both management and clerical resources and is likely to be very hectic. Even so, devoting extra time for file cleanup is well worth the effort.

Manual file conversion strategies include the following:

- Manual conversion prior to new RMS operation using existing personnel.
- Manual conversion using temporary clerks to supplement existing personnel.
- Partial conversion of files with parallel operation of old system. In this strategy, inquiries to the new RMS that find no match are referred to a clerical section that has access to the old RMS files. The old RMS information is then "cleaned up" (e.g., address is verified) and entered into the new system at the time of inquiry.

File conversion parallels preparation for RMS conversion so updates to the old RMS file must be applied to the new RMS files that are in the process of being converted. One strategy is to convert old files as of a fixed date and capture all transactions after that date for updating the new RMS just prior to its startup.

For a small agency, there is no shortcut when transitioning from a manual filing system. The files will need to be clerically entered into the new RMS.

5.9 Develop Test and Acceptance Plan

The agency will participate in testing the RMS as it is being developed, in the case of a customized system, or as it is being configured and tailored, in the case of a COTS system. Observing and/or participating in testing allows the agency to detect problems and concerns as early in the development process as possible rather than waiting for the final acceptance test. Seeing the system during testing provides the opportunity to make minor tweaks and gives insight as to how the system will actually operate.

Vendors conduct different kinds of tests, including module testing, integration testing, and final system testing. Usually they conduct their testing at the vendor's plant before the system is delivered to the agency. However, if the software operates on an agency's desktop computers, verification of early versions of the software might be possible during development. Acceptance testing is conducted at the agency, which ensures that the system truly meets the agency's needs in its own environment.

5.9.1 Integration Testing of Tailored RMS

Basic RMS software is almost always tailored by the vendor to meet each agency's unique requirements. For example, the agency name is placed on screen banners, form fields are in preferred locations, reports are specifically formatted, etc. Agencies may want to observe integration testing and final system testing at the vendor's plant. During the testing, agencies should verify the system design in these areas:

- **Modules.** If an agency is purchasing more than one module from the vendor (e.g., Case Management Module plus basic RMS), integration testing of these modules should be observed to ensure that they interact properly and their interactions are fully understood.
- **System Interfaces.** If interfaces to other systems are specified, agencies should observe how the interface software is being tested. Has the vendor set up files or other networked computers to simulate the other systems to which the RMS must interface? Do the interfaces conform to the ICDs?
- **User Interfaces.** The vendor will tailor the user interface for each agency. This custom interface should be observed and tested before RMS delivery in case adjustments to the system or procedures are necessary. For example, agencies can verify that officers are recording incident information in the format expected by the RMS.
- **Hardware Integration.** If agencies are acquiring the processor separately from the RMS software (or if an existing processing suite is being used), it is crucial to ensure that the new RMS operates effectively on the new hardware. In particular, agencies must test response time under peak conditions to ensure that the processing platform is adequate before live operation begins. This testing should use desktop and mobile data computers identical to the ones that the agency will use during live operation.
- **Communications Integration.** Integration testing should include testing of communications links identical to those that the agency will use during production operations. For example, remote access connections to the agency's local area network should be tested.
- **Other Tailoring.** All other tailoring should be verified before acceptance testing is performed.

- **NIBRS Reporting.** Agencies should ask for a specific demonstration of the RMS's NIBRS reporting capabilities during one of the early tests, and make sure that all aspects of NIBRS reporting are present and meet mandatory requirements.

5.9.2 Testing Customized RMS Modules

If the RMS is customized, the agency must be an active participant in all testing, including the customized module testing, to ensure thoroughness and proper functioning of the customized features. Additionally, agencies should require the vendor to conduct a walk-through of the customized software. Experienced software staff are needed to conduct the walk-through.

5.9.3 Acceptance Testing

Acceptance testing is conducted at the agency after the system has been installed and thoroughly checked out by the RMS vendor. This test ensures that the system meets all requirements and is acceptable for operation. During the test, the agency runs the system through its full set of functions and capabilities under peak load conditions. The test is extremely important. Acceptance of the system has strong contractual implications for the agency. Depending on how the contract is written, there may be little recourse if the agency finds problems after acceptance testing is successfully completed. *Some agencies recommend withholding final payment until live production data is successfully submitted.*

5.9.4 Test Plan

Agencies should develop a test plan with the RMS vendor, making sure the agency's priorities are a part of the plan. This means that agencies should have a strategy in mind before sitting down with the vendor. The test plan defines all tests to be performed and the agency's role in each one. For example, agency staff may act as observers on some tests and as active participants on others. Agency staff can be active participants by preparing test data or by using one of the desktop computers during the test. The plan also defines when each test is conducted and the specifics of the test. For example, the agency should determine if system interface testing includes a simulation of the system with which the RMS will interface. Specifics such as who will develop test scripts should be included.

5.9.5 Test Preparation

The agency should prepare carefully for the tests and for the participation of staff in testing. Preparation for the acceptance testing requires the most time. It is important for the agency to take as much time and invest as much effort as needed

to ensure that the system is operational and meets the agency's requirements. Test scripts must describe the step-by-step procedure to be followed during the testing. Also, test data should cover the full range of transactions and conditions to be supported by the RMS. For example, an agency could develop a stack of Incident Reports to be entered into the system by officers and/or clerks. These reports should have deliberate errors in them to verify that the RMS catches the errors and interacts properly with the person entering the information to correct the mistakes.

For a small agency, the software will probably be the vendor's standard product line with some minor tailoring. Smaller agencies may not need to visit the vendor's plant as long as the vendor agrees to correct all tailoring mistakes before the RMS is accepted. Agencies should plan on running an acceptance test; not only will this provide assurance of the product's correctness, it will also give agency staff an excellent exposure to the RMS operation.

If agencies participate in integration testing at the vendor's plant, some of the materials developed for those tests may be useful for acceptance testing as well.

5.10 Develop Training Plan

Training and retraining of an agency's staff in the use, maintenance, and operations of the new NIBRS-compliant RMS are vital to the success of the program.

5.10.1 Training Staff

All agency personnel who will interact with the new RMS and be involved at any level with NIBRS reporting must be trained on the system and/or on NIBRS. This extends from patrol officers to the police Chief, who may receive periodic reports generated by the system. It may also include personnel from other agencies that have access to system files. For example, if an agency provides processing support to another agency, their personnel must be trained.

5.10.2 The Training Plan

The training plan describes the level and extent of necessary training. Training is broader than the RMS because it is based on the new business processes defined for the new RMS and NIBRS reporting (see section 5.10.2). It encompasses new policies and procedures as well as new forms. Not all personnel should receive the same training. For example, patrol officers will receive training on the new form and procedure for recording information for the NIBRS-compliant RMS, but personnel responsible for NIBRS reporting will receive in-depth training on report preparation and quality control.

RMS vendors provide a certain amount of basic training on the RMS itself. These sessions are usually viewed as "train-the-trainer" sessions. Agencies must supplement these sessions with training on the revised policies, procedures, and forms. Agencies also must identify who their trainers will be. Depending on the agency's business processes and the selected RMS, training may be available from reputable third-party contractors.

For a small agency, the project manager will want to supplement the RMS vendor training with materials on NIBRS as well as new policies, procedures, and forms. There should be at least three people who are fully aware of how to use the system to help cover in cases where one or two key personnel may not be available.

5.11 Monitor Vendor Performance

The selected vendor is responsible for providing a system that will be the key to an agency's successful operations for years to come. Agencies should make sure that the vendor is performing as promised—agencies should not simply assume that "everything is okay." RMS vendors are like other software businesses; sometimes they over-promise or over-book and miss delivery dates, and sometimes their employees do sloppy and/or incomplete work, and some go bankrupt. Discussions with other agencies can help determine RMS vendors that have presented problems in the past.

For a small agency, the state UCR program may provide a list of vendors that have been proven to be NIBRS-compliant and meet the state's reporting needs. Make sure those vendors are invited to bid on the RMS. Track vendor progress regularly.

Participating in testing is one of the most effective means for monitoring vendor activity. In addition, agencies should ensure that deliverables such as test plans, training plans, ICDs, database schema, etc., are specified. Agencies should make sure that the deliverables are received on time, that they are quality products, and that they are specific to the agency. The vendor's financial condition should be fully investigated during source selection. The contracting office should have an ironclad contract to help ensure that the agency gets what it wants (see section 6). It is appropriate to include penalty clauses.

Finally, agencies should conduct periodic reviews with the vendor to talk over their progress and discuss any problems they may be having. If the vendors are having problems, agencies can then work with them to help solve the problem to everyone's satisfaction. Both the agency and the vendor share the goal of successful NIBRS-RMS installation.

5.12 Implementation Planning Lessons Learned

The following list contains "lessons learned" and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Agencies should refer to this list for practical advice that can be used in conjunction with the items specified in this section of the handbook. Comments from NIBRS-RMS vendors have been included where appropriate. The comments in this list do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor community.

Lessons Learned from Agencies:

- Keep all people/staff informed about NIBRS throughout process in order to keep it on their minds (talk about it at every management meeting, give presentations and Q&A sessions, write a NIBRS article in the daily/monthly bulletin, hold preliminary classes/training).
- State level criminal justice system (including crime reporting) works well because local agencies cooperated in its development.
- Remember, contractors cannot solve all your problems.
- Understand the system.
- Must have a spokesperson that keeps this issue out in front of everyone.
- Include actual, real users in the process.
- PLAN, PLAN, PLAN.
- Look for NIBRS-compliant RMS, but use caution—some vendors say they are NIBRS-compliant, but are not.
- We were already IBR, but our forms changed primarily because we went to on-line entry of Incident Report on the MDCs.
- The agency had to manually enter name and address information into new RMS to meet new system's database requirements—we had not counted on this.
- We designed the NIBRS Incident Report form first, then selected an RMS vendor—should have done the opposite.
- On initial conversion to NIBRS from Summary UCR, a large report back log with the state developed since they don't accept any IBR errors, and staff learning curve was long—during this time, crime analysis was inaccurate because data was old.
- The entire agency must be involved in, and trained on, the new RMS and NIBRS.
- Allow for lots of refresher training. Even after 2 years, a lot of mistakes are still made.
- It takes twice as long to train new recruits versus existing officers.
- Develop test data early to test and play with the system before implementation.
- Do "Report entry, edit and correction" right the first time, then IBR will reduce time and there will be more data available… otherwise there will be some negative impact due to time increase and messy data.

- Get most vocal end users to beat up on the system… you'll get negative criticism/comments however this can produce significant points early on.
- Have a lot of patience in training… takes time to refocus end users to a new reporting concept.
- Need training to offset labor-intensive elements of IBR. It takes more time to enter data but training will keep this in check.
- If the "NIBRS person" in the agency is also a sysadmin, is responsible for keeping the network going, and has other duties, it is difficult to multi-task and stay on top of NIBRS… need a person dedicated to NIBRS, but in government this may be difficult for some agencies.
- Send RMS person to training on the technology used in the vendor's product (e.g., Oracle).
- Practice, Practice, Practice during training.
- Be prepared to cater your training, because NIBRS will require re-training officers and staff, and will require continual explanations.
- Don't implement too fast. Do not implement a new CAD, new RMS, and other systems all at the same time.
- Held two training sessions for squad on how to use the IBR form. Made help-sheets that described each field and how it is to be filled out.
- Make sure officers, staff, and management are working together toward the common goal.

Lessons Learned from States:

- Don't sign off on anything with the vendor until you're fully satisfied with the product.
- Assemble a committed staff/team.
- Dedicate resources and staff to RMS processes.
- Focus on major agencies first in state, then smaller agencies (to get buy in).
- Don't develop too many ways for agencies to report (e.g., paper, tapes, BBS, etc) then expect them to go to IBR… limit their reporting options.
- Develop a state-level incident form that can be distributed to agencies for use in the field.
- State program works with both the agency and vendor to ensure that agency's RMS meets the required x% error rate.
- Look at all aspects of the RMS and make sure it is "user-friendly" for all potential users of the system.
- State provides sample forms to agencies.
- Formed a state-level committee to discuss how to address non-performing vendors.

Vendor Comments:

- Agencies need to realize and accept that their culture will be changing with the new RMS.
- Put an experienced full time person in charge of training—this should be someone who is computer-literate.

- The agency will require sufficient staff if the system is going to work—one big cause for failure is not enough of the right kinds of people involved in system implementation and operation.
- Some states provide NIBRS error-checking software to the agencies so that the reports flowing to the state have fewer errors.

CHECK LIST FOR IMPLEMENTATION PLANNING AND MANAGEMENT

- ❍ **Establish implementation team. Get dedicated time commitments.**
- ❍ **Prepare and Manage Implementation Plan**
- ❍ **Prepare and Maintain Risk Management Plan**
- ❍ **Prepare Operations and Maintenance Budget**
- ❍ **Hold Periodic Implementation Team Meetings**
- ❍ **Plan and Manage System Security**
  - **Processor and Communications Security**
  - **System Availability**
  - **Physical Security**
- ❍ **Develop Interface Control Documents**
- ❍ **Convert Files**
- ❍ **Develop Test and Acceptance Plan:**
  - **RMS Integration Testing**
  - **Testing Customized Modules**
  - **Acceptance Testing**
  - **Test Plan**
  - **Test Preparation.** Scripts, test data, etc.
- ❍ **Develop Training Plan**
- ❍ **Monitor Vendor Performance**
- ❍ **Notes and Comments:**

6 INSTALL RMS

This section describes the agency's activities associated with installing a new RMS. Section 5 describes the planning and management activities for RMS installation and NIBRS conversion, and section 7 addresses the steps to be taken to prepare the agency's staff and business processes for NIBRS reporting and for using the new RMS.

The activities described are more appropriate for a larger agency with a more complex system implementation. Small agencies should address most of these areas, but in a more simplified manner.

Outsourcing. The activities in this section assume that operation of the RMS is not outsourced to another agency or entity. If RMS operations are outsourced, these activities will be performed by the outsourcing entity.

System Integration Contractor. For larger agencies with complex systems, a system integration contractor becomes the single source for help and answers. An integration contractor could perform many of the activities described in this section.

RMS installation involves the following steps, each of which is described in this section.

- Site Preparation and Processor Installation.
- Prepare for System Operations.
- System Maintenance.
- Train Operations Staff.
- Oversee Integration Tests.

6.1 Site Preparation and Processor Installation

This section describes the activities necessary to ensure successful installation of the RMS processor and its communications links. The extent to which these activities are necessary depends on the size of the planned RMS operation. The following activities are pertinent to larger or more complex operations, e.g., RMS with LAN.

For a small agency that plans to operate on a stand-alone personal computer, this step will be fairly straightforward. There must be an adequate office working space in which to place the processor so that agency personnel can access it. However, the system should be physically placed so that non-agency personnel cannot reach the system; the agency should observe system security. The system should be plugged into a surge protector, and if the system has a modem with which to access the state message switch or any other system, then the processor should be within 30 feet or so of a phone line. A UPS will ensure continuous operation in case the power goes out.

6.1.1 Physical Plant Upgrade

The RMS processor configuration should be located in a place that can be secured with limited access control. Only authorized personnel should have access to the main processing system, for example, those personnel responsible for maintenance of the RMS. For some agencies, this may require a separate "computer room." An agency's existing computer room must be assessed to determine its adequacy for locating the new processor configuration. The agency should consider the following factors when selecting the processor's location:

- **Floor Space.** The RMS vendor (or hardware vendor if the processor is purchased from someone other than the RMS vendor) can indicate how much floor space will be needed for the RMS configuration. Space requirements should include (1) the RMS configuration, printers, data storage devices, a UPS and temperature control equipment; (2) service access to the equipment; (3) storage of spare parts; (4) supplies (paper, ink cartridges, etc.); and (5) operations personnel (desks, table space and any storage requirements for operations records and logs). If an agency has a complex system with multiple processors and components, a raised floor configuration may be needed so that cabling between the components is not in open sight. This helps prevent damage to cables and tripping by staff and gives a nicer appearance to visitors.
- **Power.** Agencies should make sure that the electrical service to the configuration is adequate, taking into consideration all peripherals that will be part of the configuration. Agencies should plan for the substantial growth of operations over a 10- to 15-year system life cycle. Vendors or hardware suppliers can provide information on power requirements. At a minimum, surge protection of the equipment is needed. However, the agency should consider a power supply that will continue to provide power for a period of time when public power service fails. If public power service is subject to frequent or extended failures, the agency should consider installing backup generators capable of supporting the main processor and some or all of the associated desktop computers. When installing desktop computers, the agency should provide surge protection for each computer. Access to these desktops should be limited to authorized staff. UPSs may be needed for a few desktop computers located near or in the computer room to allow minimum operation in case of public service power failure.
- **Heating, Ventilation and Air Conditioning (HVAC).** Today, most computers can operate in normal office environments. Even so, the agency should consider the heating and cooling requirements for the RMS configuration. This is especially true if an agency uses a closed room to house multiple, high-performance processors with power-consuming peripherals such as high-speed printers. Again, the vendor should be able to determine HVAC needs.

6.1.2 Data Communications Upgrade

The communications links to the RMS should be upgraded to accommodate the new operating mode. Agencies should consider the communications paths from the MDCs and desktops to the main system, and the communications paths to other systems with which the RMS is to communicate. For each link, the agency should consider following factors:

- Peak workload.
- Required bandwidth.
- Reliability.
- Security.

Agencies should have a professional communications engineer, review their communications system, particularly regarding security. There is a good chance that the RMS vendor does not have this kind of expertise on its staff, so agencies need to seek support from their communications providers, county or state; they may have standards and guidelines for communications. It would be wise for the agency to have an outside consultant help develop and review any plans.

6.2 Prepare for Systems Operation

The RMS requires support to keep it functioning properly. Before beginning live operation, agencies should identify the individuals or entities responsible for each function. The level of support depends on the complexity of the operation. Some of the key operating functions are described below. An agency may not have a requirement for some of these functions, or the same person may perform all the functions. Depending on the configuration, operations staff may need to be available 24 hours per day to ensure continued services, such as replying to MDC inquiries.

For a small agency, the functions listed in sections 7.2.1 through 7.2.4 should be performed by an employee or by a part-time, on-call contractor.

6.2.1 System Administration

Business computer systems require a system administrator that performs these kinds of functions:

- Applies upgrades to the software.
- Schedules and performs periodic backup of the system.
- Recovers RMS data when files are lost.
- Adds new users to the system.
- Monitors operating characteristics to ensure that performance, such as user response-time is reasonable.
- Applies system patches and ensures that information security mechanisms are implemented and maintained.

- Maintains viable operations links to the MDCs and other agencies with which the RMS communicates.

For larger agencies, this may involve full-time staff or a part-time person, depending on the size of the computer operation. The person may be an employee or could be a contractor. If an agency chooses to outsource, this service would be provided by the outsourcing entity.

6.2.2 Security Administration

An agency should assign one or more well-trusted persons who have the responsibility for ensuring security of the RMS and its data and other related systems, such as network systems. In simpler operations, the security administrator function may be assigned to the system administrator; however, larger agencies will want specially trained employees performing this function. This function becomes even more important and more complex in more complex operations, particularly in those that have communications between the RMS and MDCs or other agencies. The security administrator will need a thorough technical understanding of system security and the RMS. Sections 2.3.1 and 6.2.2 describe the security functions to be performed by the security administrator.

6.2.3 Configuration Management

More likely than not, the RMS will be upgraded or modified over time. Software upgrades, new reporting requirements, replacement of hardware components, or modification of communication services are typical changes which affect an RMS or one of the systems with which it interacts. Each of these changes can impact more than one component of the system, and some changes are contingent on prior changes being made. For example, a software upgrade may require an upgrade to the processor's operating system. Even with a stand-alone desktop computer at a small agency, modifications or upgrades are likely.

Configuration management uses a systematic approach to keep track of the components of the system and how they relate to each other. It ensures that as changes are made, the system will continue to operate. The more complex the system, the more complex configuration management becomes. One person must be responsible for configuration management of the entire RMS and its connecting systems. This person should keep records of changes and enforce testing to ensure system stability prior to the application of each change. Configuration management software packages can be used to help perform this function.

6.2.4 Help Desk

This function provides support to users of the system by answering questions when users are not able to use the RMS, reasons such as software bugs,

communication link failure, processor failure, etc. The larger the operation, the greater the potential for such problems. Help desk personnel must understand how the system operates and keep track of problems and solutions so that they are prepared to give assistance when needed. The help desk could be staffed by an agency's own personnel, with contacts for vendors (hardware, RMS, and communications) to help answer the tougher questions. The help desk may be a 24 x 7 hour operation for some agencies.

In the initial stages of operation with the new system, this function is vital as users who have just finished their training courses forget the details of operation. Agencies may also choose to have the help desk answer policy and procedure questions for patrol officers. This is particularly helpful for agencies in the initial stages of incident-based reporting or when patrol officer procedures have changed.

6.3 System Maintenance

One of the vendors performs maintenance. In some cases, a fixed amount of maintenance comes with the system; vendors charge fees for any additional service. During source selection, agencies should obtain a complete statement of what is and is not included. Maintenance contracts generally include the following:

- **RMS Software.** The RMS vendor maintains RMS software. If the RMS has been customized, RMS vendors charge an additional fee to maintain the customized software unless the agency itself has a proficient programming staff and the customization is a separate module.
- **Processing Suite.** The processing suite includes all hardware components, such as computers and printers, and system software components that were provided with the hardware such as the operating system.
- **Other System Software.** If system software was acquired beyond that provided by the processing suite vendor, such as a database management system or virus protection, then the company that sold the software is responsible for correcting faults and providing upgrades to the software package.
- **Communications.** This involves one or more vendors. For example, if a local telephone company provides a link to both the MDCs and the building's communications system (e.g., a PBX or local area network), all three vendors provide maintenance related to communications.
- **Miscellaneous.** If agencies have a UPS or special heating or cooling units, their maintenance is provided by different entities.

When a failure occurs in a complex system, it is often difficult to pin down exactly where it occurred. Self-diagnostic software can be installed to continually test the various components to help provide some answers. Maintenance personnel can sometimes help. For a more complex system that requires different

kinds of maintenance agreements, agencies need a staff member who is an expert on the system and understands how each component contributes to its operation.

6.4 Train Operations Staff

The operations staff performing the functions described thus far must be trained. Even if an agency already has a data processing center, there will be new procedures and information that must be learned. Vendors provide most of the necessary training to operate the new system. Other training could involve classes at trade schools on new equipment or components.

Training makes employees more valuable in the job market. In particular, salaries in the IT market may be higher than an agency normally offers. Technical staff members are likely to look for job advancement opportunities and promotions commensurate with other entities. Agencies work with their human resource department to establish a plan to retain technical staff. If it is difficult for an agency to train its staff or retain them, then the agency should consider the use of contract personnel for operating the system.

6.5 Oversee Integration Tests

Operations personnel lead the agency's observation of the vendor's system integration tests, as described in section 5.9.1. These tests allow the operations staff to address some of their more serious concerns early in the development cycle. It also gives them an opportunity to become acquainted with the vendor's policies, procedures, and personnel. This is very helpful during system implementation and operation.

6.6 RMS Installation Lessons Learned

The following list contains "lessons learned" and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Agencies should refer to this list for practical advice that can be used in conjunction with the items specified in this section of the handbook. Comments from NIBRS-RMS vendors have been included where appropriate. The comments in this list do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor community.

Lessons Learned from Agencies:

- Must have a spokesperson that keeps this issue out in front of everyone.
- Should get help from vendor (or someone) in site preparation (e.g., running cable, etc.).
- The agency had to manually enter name and address information into new RMS to meet new system's database requirements—we had not counted on this.

- After RMS is acquired, make sure you understand the system's tables and operation BEFORE entering any data.
- It's difficult to keep up with edits (QC), which creates a backlog, so it's best to have dedicated staff.
- Be patient… it takes a while to adapt.
- IT staff must understand the RMS.
- Used volunteer workers during initial IBR operation to review officer entries.

Lessons Learned from States:

- Assemble a committed staff/team.
- Dedicate resources and staff to RMS processes.
- Training is very important to Quality Control.
- Establish a stringent audit program.
- Software package provided to each agency by State; they use this to edit their NIBRS reports before sending to the state; it helps them find out where their problems are.

Vendor Comments:

- The Systems Administrator must understand NIBRS completely.
- Management must be proactive and watch the implementation closely to ensure it stays on track.
- "Tweaking" during implementation can cause delays.

CHECK LIST FOR RMS IMPLEMENTATION

- ❍ **Site Preparation and Processor Implementation.** Prepare for RMS computer configuration and install it:
  - **Physical Plant Upgrade.** Floor space, power, HVAC, etc.
  - **Data Communications Upgrade.** Assess communications channels.

- ❍ **Prepare for Systems Operation**
  - **System Administration.** Person to apply software upgrades, schedule and perform file backups, etc.
  - **Security Administration.** Person to maintain system security, grant approval for access, etc.
  - **Configuration Management.** Keep track of hardware and software patches and upgrades, ensure system operability.
  - **Help Desk.** Provide support to system users.

- ❍ **Prepare for System Maintenance:**
  - **RMS Software**
  - **Processing Suite**
  - **Other System Software**
  - **Communications**
  - **Miscellaneous**

- ❍ **Train Operations Staff**

- ❍ **Oversee Integration Tests**

- ❍ **Notes and Comments:**

7 AGENCY PREPARATION

This section describes the agency's preparation of staff and business processes for use of the new RMS and NIBRS reporting. This activity begins when the decision is made to proceed with NIBRS and RMS acquisition. It parallels RMS definition, acquisition, and installation. This activity ends after the agency's RMS acceptance test and conversion of the agency to NIBRS and the new system.

The activities described are more appropriate for a larger agency with major changes to its business practices. Small agencies should address most of these areas, but in a more simplified manner. For each area, the potential activities for a small agency are described.

Outsourcing. An agency should perform all of these activities even if it outsources the system's operation. A systems integration contractor could help the agency perform some of the activities.

Agency preparation involves the following steps, each of which is described in this section:

- Document Current Business Flow check (also pp. 3, 6, 35).
- Develop New Business Flow with NIBRS.
- Revise Policies and Procedures.
- Redesign Forms.
- Conduct RMS Acceptance Test.
- Prepare Each Operating Unit.
- Train Users.
- Convert to New System.

7.1 Document Current Business Flow

If an agency has not already documented its business flow during the normal course of business, then the agency should do so before it can prepare itself for the impact of a new major system. This is the only way an agency can define how its business practices will change. Many agency managers who do this are surprised to find that there are aspects of their operation that they did not fully understand.

Documentation involves writing down the step-by-step procedures that are followed by personnel in the areas affected by the new RMS. This can be a simple list, or it can involve a chart showing how information flows through the process. To help ensure

For a small agency, documenting current business flow may help with understanding and accepting the new procedure that will need to be followed with the new RMS.

accuracy and completeness, it may be wise to have this process documented by someone trained in business procedures, rather than by immediate supervisors.

7.2 Develop New Business Flow with NIBRS

Agencies should describe how information will flow and how functions will be performed. The RMS vendor and other agencies that are using the vendor's product can help. If an agency is moving to an incident-based reporting from Summary UCR, this requires documenting the new information flow and functions at every level. This is particularly true if an agency is moving to MDC use to record reports in the field. For example, agencies should be aware of new editing and quality control functions that will be performed with NIBRS and the new RMS. Specific considerations include the following:

- Information flow and function of each operation affected by the new RMS and by NIBRS reporting.
- Impact of state reporting requirements on NIBRS report preparation.
- Data-entry-level editing of incident or offense reports.
- Quality control of reports in the RMS.
- Procedures to access the RMS.
- RMS reports and their distribution.
- Interactions with a geographical information system (GIS) for reporting and analysis.

Agencies should compare the new workflow to the existing procedure to identify necessary changes. Changes may include redistributing functions, approvals, and information flow. These changes most likely will impact an agency's procedures and form designs. Agency policies may also be affected.

For a small agency, procedures will change. These changes need to be developed and documented.

7.3 Revise Policies and Procedures

Policies. An agency's policies may need to change for operations with the new RMS and/or for incident-based reporting. This is particularly true if the adoption of NIBRS is accompanied by a move to file reports via MDC. Once the agency has a vision of how incident-based reporting impacts each department, it should establish a policy review committee.

Procedures. An agency's procedures will change, both for incident-based reporting and for the new RMS. As previously noted, these changes will be defined by the new business flow. Agencies should document these procedures, but it is a good idea to first do a dry run of each procedure to make sure it is reasonable and workable. The dry run gives the staff a glimpse of how the new system will impact their operations.

7.4 Redesign Forms

As an agency moves from Summary UCR to NIBRS, new information should be recorded. Agencies will probably want officers to enter incident and arrest information into a computer-based suspense file via MDC or desktop computer. It is important to ensure that all information necessary for NIBRS, the agency, and the state is recorded by the responding officer as soon as possible.

For a small agency, forms redesign will be necessary, particularly when moving to incident-based reporting.

The new RMS will prompt the officer for information, and the system can edit each entry as it is being keyed. Some agencies may decide to have the officer record paper reports for clerks to enter into the system at a later time. This approach is not encouraged because the clerk has to contact the responding officer to resolve any questions arising from data entry edits. Supervisors will then have to pull the reports from the suspense file and review and approve them using desktop computers. Some agencies may choose to have NIBRS clerks review each report to determine if the report is as correct as possible before it is moved into the RMS files. Other agencies will want to wait and have the NIBRS review occur the next day.

The decision on which approach to follow affects both policies and procedures. If the RMS uses on-line data entry, incident and arrest forms are printed on the computer after supervisor approval; this is the only way to obtain the report in paper form under this approach.

Redesign must be consistent with computer printouts and vice versa. Agencies should have paper incident and arrest forms to manually enter information when the officer is not immediately able to enter data into the computer. Those forms should be identical to the computer-generated forms.

The officer should sign the form before it is forwarded to the prosecutor's office and the courts, and the signed form is considered the report of record. Some states are looking into the use of *electronic signatures*. This would mean that the computer version of the form would be forwarded to another department's computer and the computer file would be considered the copy of record for archiving. This kind of change, while desirable from a systems point of view, requires the agreement of the community's (and perhaps state's) criminal justice system, including courts, prosecuting and defense attorneys, corrections, etc.

7.5 Conduct RMS Acceptance Test

The RMS acceptance test, which is the final test of the system prior to its official turnover to the agency, is conducted after the system has been installed and thoroughly checked out by the RMS vendor. **This test ensures that the system meets all of the agency's requirements and is acceptable for operation.**

Acceptance testing is extremely important. The formal acceptance of the system by the agency has strong contractual implications. If an agency does not express any concerns about the system within the contractual time limits and in the prescribed manner, the system is deemed acceptable for operation under the terms of the contract. Problems discovered after the system has been officially accepted by the agency must be dealt with under contracted maintenance and warranty agreements.

For a small agency, acceptance testing is critical. All testing should be thorough. Smaller agencies may need help from another agency in developing the scripts and test data. This will give staff an opportunity to work with the new system.

Therefore, acceptance testing should heavily involve the staff that will be using the system. They must run the system through its full set of functions and capabilities under peak load conditions. Ideally, every requirement in the RMS specification that was prepared should be tested during acceptance testing. Agencies should take their time and make sure the test is thorough.

It may be unrealistic to expect everything to work perfectly during acceptance testing. Agencies may want to set up a scoring system in which critical functions are weighed more heavily than less critical ones. Acceptance criteria can be defined from the scoring system. For example, an agency might define its key operations as critical, and not accept the system until fully functional. On the other hand, a banner that does not have the agency's logo on it is not as important. The vendor can correct that after the testing is complete.

Acceptance testing must be well planned. Scripts must be prepared for each function to be performed, and test data must be prepared so that simulated files can be accessed and updated, simulated incident and arrest reports can be entered and edited, etc. The annual reporting cycle of NIBRS should be simulated and incorporated into acceptance testing so that the staff gets a sense of the editing and quality control functions to be performed. The acceptance test will be complete if NIBRS error checking capabilities, i.e., edits, are thoroughly assessed. This can be done by a few months of live data entry from which files are generated and sent into the state-certified repository to see if the agency software finds all of the errors that the state repository finds. The state can send this data on to the FBI to see if any other gaps are identified in the NIBRS error-checking of the RMS.

7.6 Prepare Each Operating Unit

Procedures and detailed instructions are needed for each operating unit in the agency that will be affected by the new RMS and/or incident-based reporting. The staff in each unit can help in the preparation. Agencies should pay close attention to details. For example, an agency may need to prepare new forms for activities such as logging work in and out of the unit. The physical space

for each unit should be reviewed to make sure its size and layout is consistent with the new procedures. For example, if the new procedures involve the use of desktop computers in areas where they were not used before, then the physical space must be adjusted to accommodate them.

For a small agency, each unit will need to be prepared as described in section 7.6.

One major consideration is the transition period. An agency may choose to implement the system in phases, for example, one district at a time. In this case, the staff in some operating units may be following old procedures parallel to new ones for a period of time.

7.7 Train Users

Training should be agency-wide and may also include training for individuals from other criminal justice agencies that may have access to the system. User training is very important. Other employees should receive orientation training—some may be able to help during the transition. Other agencies that will receive new reports or forms from the system should also receive some level of training or orientation. User training should occur as close to the actual start of the new system use as possible so that the training is fresh in the staff's mind when the new operation begins. Training followed by simulated hands-on use of the system and/or participation in acceptance testing is most effective. In this way, early feedback can be obtained on any procedural problems or areas where training needs to be bolstered.

For a small agency, proper training of staff is critical. All agencies should take the time and effort to conduct appropriate training.

Vendors generally *train the trainer*, i.e., provide training for one or more people as designated by an agency, usually staff members (but sometimes contractors), who in turn conduct the training at the agency. Agencies should supplement the training curriculum with specifics about operations, policy and procedure changes, and form redesign. Plans for training should incorporate periodic retraining sessions in addition to training new employees.

7.8 Convert to the New System

Conversion to the new RMS should be planned in detail. A pilot conversion of a single function and/or a single location allows an agency to gain a sense of the problems that could be encountered when the entire agency converts. Beyond the pilot, it may be a good idea to use a phased conversion strategy. An agency may want to convert one function at a time, for example, convert incident reporting first and convert arrest report preparation later, or convert property management after case management. A stepped conversion allows the agency to manage

more easily the problems that might arise (people forget procedures, system needs adjustments, etc.). It also allows the agency to conduct training in phases so that classes are smaller and the curriculum is more focused.

For a small agency that is converting from a manual system, the easiest conversion approach may be for staff to work over the weekend and convert to using the new RMS. However, agencies should make sure to perform a dry run of the operation before attempting to do this.

As conversion progresses, it is important for the agency management to closely monitor the system's acceptance and effectiveness. Executive and project managers should know if the project is meeting its goals, particularly those that helped justify the new RMS.

7.9 Agency Preparation Lessons Learned

The following list contains "lessons learned" and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Agencies should refer to this list for practical advice that can be used in conjunction with the items specified in this section of the handbook. Comments from NIBRS-RMS vendors have been included where appropriate. The comments in this list do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor community.

Lessons Learned from Agencies:

- City council must be prepared to see different (perhaps higher) crime statistics numbers so there is no negative reaction.
- Must have a spokesperson that keeps this issue out in front of everyone.
- Dedicate staff to the team full-time, and include staff/input from all impacted users (e.g., courts).
- Must create NIBRS experts within your agency.
- Our move to NIBRS coincided with move to MDCs, so that crime classification on Incident Reports is now done by field officers who are given pull-down menus and prompting; the officer training for this should have been more fully considered. We have had to add a back-end editing function to verify codes as officers learn crime classification.
- For an agency moving from Summary UCR reporting (no IBR) lots of officer training and retraining and experience needed for them to learn which are NIBRS versus non-NIBRS events.
- Comparing Summary UCR to NIBRS, must account for the fact that it takes longer to prepare an Incident Report, enter the data and back-end edit it—the Report is much longer and more complex (our old offense report was 1 page, now it is 8 pages).

- On initial conversion to NIBRS from Summary UCR, a large report back log with the state developed since they don't accept any IBR errors, and staff learning curve was long—during this time, crime analysis was inaccurate because data was old.
- The entire agency must be involved in, and trained on, the new RMS and NIBRS.
- Develop test data early to test and play with the system before implementation.
- There will always be more that you could have done.
- Accept that it will be obsolete when you go live.
- The RMS is never finished.
- It's difficult to keep up with edits (QC), which creates a backlog, so it's best to have dedicated staff.
- Communicate with management as project progresses. "Sell" NIBRS at every chance.
- Be patient… it takes a while to adapt.
- Dedicate a person in records staff to overseeing the quality of NIBRS data.
- Training on the NIBRS-RMS should be about what officers and staff are going to be doing everyday. Agencies shouldn't clutter up staff with all the bells-and-whistles and with the technology stuff. NIBRS is complicated, so don't get too detailed in your training.
- Train-the-trainer doesn't always work so well… sometimes it's better to just go ahead and set aside 3-day sessions that staff are required to attend.
- Train road-sergeants and supervisors ahead of time, not in the middle of the process.
- Training should be held close to implementation time, then "let them loose" on the actual computers, then follow-up with more training.
- Sometimes NIBRS logic doesn't jibe with your own logic… don't get hung up on that.
- Held two training sessions for squad on how to use the IBR form. Made help-sheets that described each field and how it is to be filled out.
- Make sure officers, staff, and management are working together toward the common goal.
- Nothing moved forward with a committee of part-time people. Implementation was done by one full-time person [agency has 50 sworn officers]. Did not start until the "last minute," so participation by officers and staff was minimal; this created problems of acceptance.
- State penal code and NIBRS are not in agreement, so the Incident Report might show "Unlawful Entry and Assault" while the Arrest Report would show "Burglary."
- Quality Assurance is a problem; clerks must correct data after it is entered into the RMS. The MDC use will correct this problem because the officer will be guided through the data entry, and auditing of the data entry can occur at the district office.

Lessons Learned from States:

- Assemble a committed staff/team.
- Dedicate resources/staff to RMS processes.
- Develop a state-level incident form that can be distributed to agencies for use in the field.
- Understand the data that you're sending in.
- It's hard, it's frustrating, and it takes a while… but the extra info and data are worth it.
- Prepare for double entry and staffing resources during transition from Summary to NIBRS.
- Agencies should communicate regularly with their state UCR representative and coordinate any system changes or upgrades BEFORE sending data through to the state. State program is there to help.
- State programs need to be sure to focus on customer service.
- States can establish annual training requirements to ensure that data quality levels are maintained.
- State provides sample forms to agencies.
- State provides 8 state troopers for NIBRS training across the state to agencies.
- Officers do not like to fill out the additional details in the forms.

Vendor Comments:

- The Systems Administrator must understand NIBRS completely.
- The agency will require sufficient staff if the system is going to work—one big cause for failure is not enough of the right kinds of people involved in system implementation and operation.
- The offense report form must be redesigned to have NIBRS-compliant data fields.
- Agency should create a group to deal with data collection and forms design in preparation for NIBRS.
- Revamp forms, procedures and workflow prior to going to computer-based system.
- Every 6-12 months, retrain personnel, and evaluate the workflow to correct any bad procedures.

CHECK LIST FOR AGENCY PREPARATION

- ❍ **Document Current Business Flow**

- ❍ **Document New Business Flow with NIBRS**

- ❍ **Revise Policies and Procedures**

- ❍ **Redesign Forms**

- ❍ **Conduct RMS Acceptance Test.** This test ensures that the RMS meets all requirements and is ready for operation:
  - **Scenarios.** These should cover all critical functions of the RMS: also system response times should be tested under load conditions.
  - **Scripts.** Prepare scripts for each test so that each tester knows what to do and when.
  - **Test Data.** Prepare files and transactions in advance so testers have a basic system with which to operate.
  - **Results Monitoring.** Maintain logs of the test so that failures and problems are specifically documented.

- ❍ **Prepare Each Operating Unit for Conversion.** Make sure each operating unit is prepared for the new RMS and NIBRS operation.

- ❍ **Train Users**

- ❍ **Convert to New System:**
  - **Phase Conversion?**
  - **Total Agency Conversion?**

- ❍ **Notes and Comments:**

Appendix A: Summary of Lessons Learned

Appendix A provides a summary of the Lessons Learned sections located throughout the handbook. The tables in this Appendix contain best practices and advice from state and local agencies that have been NIBRS-certified or are implementing NIBRS-compliant RMSs. Comments from NIBRS-RMS vendors are also included. The respective handbook section(s) is indicated for each comment in the tables. This summary of practical advice can be helpful to agencies in navigating sections of the handbook. The comments in these tables do not constitute statements from the FBI or BJS; comments are entirely from the NIBRS user and vendor community.

Table A.1 Agency Lessons Learned Summary

Agency Lessons Learned	Referenced Handbook Section						
	1	2	3	4	5	6	7
Don't be afraid to change things to get to NIBRS from the old ways of doing reporting/business . . . Have an open mind.	X	X					
Keep all people/staff informed about NIBRS throughout process in order to keep it on their minds (talk about it at every management meeting, give presentations and Q&A sessions, write a NIBRS article in the daily/ monthly bulletin, hold preliminary classes/training).	X	X			X		
Acquiring and implementing NIBRS-RMS will be the most complex project that the agency will ever do.	X	X					
Talk with other agencies. Go onto the Internet	X	X					
Conversion to NIBRS is much easier if your agency and state already have incident-based reporting.	X						
State level criminal justice system (including crime reporting) works well because local agencies cooperated in its development.	X				X		
Comparing Summary UCR to NIBRS must account for the fact that it takes longer to prepare an Incident Report, enter data and back-end edit it—the Report is much longer and more complex (our old offense report was 1 page, now it is 8 pages).	X						X
Your planning needs to account for the fact that initially it will take a lot more officer time and more back office editing time as their learning curve increases; it will level out, but still be more than what it was if you did Summary UCR before.	X						
Smaller agencies do not have as many incentives to go to their own system; they could be supported more by the state, or perhaps be serviced by a larger agency.	X						
Need full commitment from the Chief and his executive staff as well as other criminal justice leaders in the community—courts, prosecutors, sheriff's, etc.	X						
City council must be prepared to see different (perhaps higher) crime statistics numbers so there is no negative reaction.	X						X
The greater length of time that it takes to complete incident reports is offset by the agency getting a better look at crime.	X						

Agency Lessons Learned (Continued)	Referenced Handbook Section						
	1	2	3	4	5	6	7
Substantial benefits in crime analysis and crime mapping.	X						
NIBRS produces better information and a more readable report.	X						
The computer will do a lot for you. Before NIBRS-RMS, a records clerk had to read every report individually.	X						
NIBRS forces better crime scene data collection and is better for reporting hate crimes. Better crime analysis.	X						
Questions by officers when completing report show victim a higher level of caring.	X						
Explore your options—depending on the complexity of your requirements and your staff, in-house development may be attractive.		X					
Spend time designing the offense report to get it right—we spent 2 years.		X					
Use of MDC with pull-down menus, prompting, and on-line editing should reduce time for NIBRS-compliant report preparation by 50%.		X					
Need a teamwork philosophy across the agency.		X					
Need to get all users involved up front.		X					
Need a business practices team to revise business flow, procedures and redesign forms.		X					
Remember, contractors cannot solve all your problems.		X			X		
Everybody needs to immerse themselves in what NIBRS is all about (really get to know what it provides and why to do it).		X					
Understand the system.		X			X		
PLAN, PLAN, PLAN.		X			X		
If you spend 18 months planning, then you can do a 6-month implementation; if you spend 1 1/2 hours planning, then you'll spend 18 years implementing.		X					
Need a full-time advocate.		X					
Get the right people involved . . . Must have Vision.		X					
Don't have a person in charge that is frightened about change; requires a leader who believes in the process/project and can instill this in others.		X					
Don't build into a dead-end situation.		X					
It is a long, tedious process, so treat it that way from the beginning . . . "Devil is in the details."		X					
Spend lots of time in preparing detailed RFP . . . Vague RFP leads to drawn out negotiations, we should have put more detail in our RFP.		X					
Must have a spokesperson that keeps this issue out in front of everyone.		X			X	X	X
Include actual, real users in the process.		X			X		
Dedicate staff to the team full-time, and include staff/input from all impacted users (e.g., courts).		X					X
Need PR within your agency.		X					
Prepare as much as possible.		X					

Agency Lessons Learned (Continued)	Referenced Handbook Section						
	1	2	3	4	5	6	7
Get your data structured BEFORE you start (tables, codes, mappings).		X					
Make sure that your agency is classifying crimes correctly in Summary, before moving to NIBRS. Otherwise, comparisons of crime rates will be "apples to oranges."		X					
Start researching for NIBRS early. PLAN!		X					
A small agency should research for 1 year before starting acquisition process. A large agency (250,000+ population served) should research 3 years before starting.		X					
Take a "NIBRS for dummies" approach as best you can. Simplify.		X					
It may be more effective for an agency's management to require "NIBRS or else" in order for the ranks to adapt.		X					
Acquire the latest technology.		X					
Make RFP very specific in what you want.		X		X			
Must create NIBRS experts within your agency.		X					X
Pay attention to how the program puts the data in the RMS. Ensure proper user-interface flow, from input to storage to reporting.		X					
Look closely at the need for custom programming; will it be covered by the maintenance agreement?		X		X			
Make sure officers, staff, and management are working together toward the common goal.		X			X		X
Nothing moved forward with a committee of part-time people. Implementation was done by one full-time person (agency has 50 sworn officers). Did not start until the "last minute," so participation by officers and staff was minimal; this created problems of acceptance.		X					X
Convince whomever gives money/funding that it is for "continuing operational expense" not for "capital expense," because you'll need the funding more than just to get started.			X				
Get twice as much money as you think you need . . . It "snowballs very quickly."			X				
Apply for many grants.			X				
Many times, grants aren't enough. Pursue capital improvement funding.			X				
Pursue civil grants that are technology related.			X				
COTS system that we purchased met NIBRS compliance but had to be customized to meet state needs, which are more extensive than NIBRS.				X			
Should get help from vendor (or someone) in site preparation (e.g., running cable, etc.).				X			
Move to NIBRS coincided with move to MDCs, so that crime classification on Incident Reports is now done by field officers who are given pull-down menus and prompting; the officer training for this should have been more fully considered—have had to add a back-end editing function to verify codes as officers learn crime classification.							X

Agency Lessons Learned (Continued)	Referenced Handbook Section						
	1	2	3	4	5	6	7
Look for NIBRS-compliant RMS, but use caution—some vendors say they are NIBRS-compliant, but are not.				X	X		
We were already IBR, but forms changed primarily because we went to on-line entry of Incident Report on the MDCs.					X		
The agency had to manually enter name and address information into new RMS to meet new system's database requirements—we had not counted on this.					X	X	
We designed the NIBRS Incident Report form first, then selected an RMS vendor—should have done the opposite.					X		
After RMS is acquired, make sure you understand the system's tables and operation BEFORE entering any data.						X	
For an agency moving from Summary UCR reporting (no IBR) lots of officer training and retraining and experience needed for them to learn which are NIBRS versus non-NIBRS events.							X
On initial conversion to NIBRS from Summary UCR, a large report back log with the state developed since they don't accept any IBR errors, and staff learning curve was long—during this time, crime analysis was inaccurate because data was old.					X		X
The entire agency must be involved in, and trained on, the new RMS and NIBRS.					X		X
Allow for lots of refresher training; even after 2 years, a lot of mistakes are still made.					X		
It takes twice as long to train new recruits versus existing officers.					X		
Check to see if the new RMS accepts mug shots so that they can become part of the RMS records.				X			
Develop test data early to test and play with the system before implementation.					X		X
Do "Report entry, edit and correction" right the first time, then IBR will reduce time and there will be more data available . . . Otherwise there will be some negative impact due to time increase and messy data.					X		
Get most vocal end users to beat up on the system . . . You'll get negative criticism/comments; however, this can produce significant points early on.					X		
Have a lot of patience in training . . . Takes time to refocus end users to a new reporting concept.					X		
There will always be more that you could have done.							X
Accept that this will be obsolete when you go live.							X
The RMS is never finished.							X
Do hands-on evaluation of vendor products BEFORE contract.				X			
Want to work with the vendor's actual developers, not just the vendor's managers.				X			
Need training to offset labor-intensive elements of IBR. It takes more time to enter data but training will help to keep this in check.					X		

Agency Lessons Learned (Continued)	Referenced Handbook Section						
	1	2	3	4	5	6	7
It's difficult to keep up with edits (QC), which creates a backlog, so it's best to have dedicated staff.						X	X
Vendor demo is not enough. Must conduct site visits and contact current users of vendor's products.				X			
Communicate with management as project progresses. "Sell" NIBRS at every chance.							X
Be patient . . . It takes a while to adapt.						X	X
Dedicate a person in records staff to oversee the quality of NIBRS data.							X
If the "NIBRS person" in the agency is also a system administrator, is responsible for keeping the network going, and has other duties, it is difficult to multi-task and stay on top of NIBRS . . . Need a person dedicated to NIBRS, but in government this may be difficult for some agencies.					X		
Send RMS person to training on the technology used in the vendor's product (e.g., Oracle).					X		
Training on the NIBRS-RMS should be about what officers and staff are going to be doing everyday. Agencies shouldn't clutter up staff with all the bells-and-whistles and with the technology stuff. NIBRS is complicated, so don't get too detailed in your training.							X
Practice, practice, practice during training.					X		
Be prepared to cater your training, because NIBRS will require retraining officers and staff, and will require continual explanations.					X		
"Just because vendor says 'NIBRS-compliant' means nothing." Make absolutely sure that vendor's product is NIBRS-compliant AND that it is capable of meeting all state requirements for certification in the particular state.				X			
Don't implement too fast. Do not implement a new CAD, new RMS, and other systems all at the same time.					X		
Train-the-trainer doesn't always work so well . . . Sometimes it's better to just go ahead and set aside 3-day sessions that staff are required to attend.							X
Train road-sergeants and supervisors ahead of time, not in the middle of the process.							X
Training should be held close to implementation time, then "let them loose" on the actual computers, then follow-up with more training.							X
IT staff must understand the RMS.						X	
Sometimes NIBRS logic doesn't jibe with your own logic . . . Don't get hung up on that.							X
Held two training sessions for squad on how to use the IBR form. Made help-sheets that described each field and how it is to be filled out.					X		X
Used volunteer workers during initial IBR operation to review officer entries.						X	

Agency Lessons Learned (Continued)	Referenced Handbook Section						
	1	2	3	4	5	6	7
RMS software was not NIBRS-compliant, but software company made changes for nothing so that their software would be certified for NIBRS reporting.				X			
State penal code and NIBRS are not in agreement, so Incident Report might show "unlawful entry and assault" while the Arrest Report would show "Burglary."							X
Quality Assurance is a problem; clerks must correct data after it is entered into the RMS. The MDC use will correct this problem because the officer will be guided through the data entry, and auditing of the data entry can occur at the district office.							X

Table A.2 State Program Lessons Learned Summary

State Program Lessons Learned	Referenced Handbook Section						
	1	2	3	4	5	6	7
Research!	X	X					
"Every week in planning saves a year later on."	X	X					
Talk to other agencies.	X	X					
Combine with other agencies in county or region to obtain a NIBRS-RMS together.	X		X				
It's a big decision and a lot of work…know why you want to do it and know what the benefits are before getting started.	X						
Each agency has a responsibilty to its state, jurisdiction, citizens, and its own agency to ensure complete NIBRS data reporting.	X						
Must talk to other agencies…learn from what they did right and from what they did wrong.	X						
It seems to take about 9 months for an agency to adjust to NIBRS; after that, agencies seem to have adjusted and seem okay.	X						
Assemble a committed staff/team.		X			X	X	X
Spend a lot of time on defining requirements/needs… BE VERY SPECIFIC.		X					
Get input from your "customers"… in other words, from agencies throughout your state.		X					
Must manage people well, make sure "all on same page."		X					
Dedicate resources, staff to RMS processes.		X			X	X	X
Identify your own needs first.		X		X			
Make absolutely sure that hardware (exsisting or new) is compatible with the software.		X					
Know what you want to get out of the system.		X					
Focus on major agencies first in state, then smaller agencies (to get buy in).					X		
Talk to other users of vendors products.				X			
Don't develop too many ways for agencies to report (e.g., paper, tapes, BBS, etc) then expect them to IBR…limit their reporting options.					X		
Develop a state-level incident form that can be distributed to agencies for use in the field.					X		X
Check out vendors with other users.				X			
Identify milestones in the contract.				X			
Put opt-outs in contract (for example., a stop work after the requirements document if you don't like it, or after system design, etc)…penalty clauses.				X			
We sent out RFQ to 7 vendors, got 5 responses. We shared our Vision with the vendors to see if they wanted to "join up."				X			
State program works best with both the agency and vendor to ensure that agency's RMS meets the required % error rate.					X		
Don't ever purchase any vendor products that are not certified/approved/ acknowledged by your state program.				X			

State Program Lessons Learned (Continued)	Referenced Handbook Section						
	1	2	3	4	5	6	7
State programs should try to do their best to get money/funding to actually help their agencies implement NIBRS-RMS.			X				
Don't sign off on anything with the vendor until you're fully satisfied with the product.				X	X		
Understand the data that you're sending in.							X
It's hard, it's frustrating, and it takes a while… but the extra info and data are worth it.							X
Don't invest a lot of money in vendors that have no NIBRS experience and are not confirmed to be NIBRS-compliant.				X			
Go after as many law enforcement grants as possible.			X				
Actually test the vedor's system before taking any further steps.				X			
Check around with other agencies to get opinions and experiences with vendor's products.				X			
Look at all aspects of the RMS and make sure it is "user-friendly" for all potential users of the system.					X		
Prepare for double entry and staffing resources during transition from Summary to NIBRS.							X
Agencies should communicate regularly with their state UCR representative and coordinate any system changes or upgrades BEFORE sending data through to the state. State program is there to help.							X
Training is very important to Quality Control.						X	
State programs need to be sure to focus on customer service.							X
Be sure that grants are for purchasing hardware, the NIBRS-RMS software, and all elements of the system, otherwise some things will be missing and the system (and you) will suffer.			X				
Establish a stringent audit program.						X	
States can establish annual requirements to ensure that data quality levels are maintained.							X
The state provides support and encouragement to agencies to convert to NIBRS with matching funding provided to local agencies.			X				
State provides sample forms to agencies.					X		X
State provides 8 state troopers for NIBRS training across the state to agencies.							X
Software package provided to each agency by State; they use this to edit their NIBRS reports before sending to the state; it helps them find out where their problems are.						X	
Vendors get certified in the state when they successfully implement a NIBRS-compliant system in the state.				X			
Most agency complaints are about vendors that did not perform lots of promises, but when problems occur, the vendor often does not support the agency.				X			
Officers do not like to fill out the additional details in the forms.							X
Formed a state-level committee to discuss how to address non-performing vendors.				X	X		

Table A.3 Vendor Comments Summary

Vendor Comments	Referenced Handbook Section						
	1	2	3	4	5	6	7
Agencies need to realize and accept that their culture will be changing with the new RMS.	X				X		
Top management as well as middle managers must buy into the modernization and openly support it.	X						
Make sure the state trains the agencies on their reporting demands and that these demands are included in the RMS specifications so that the new RMS software does not get blamed when reporting is wrong.		X		X			
Data entry people must be trained . . . they can't make as many errors as they might have with Summary UCR report preparation; edit checks in the software help catch some mistakes.		X					
Agency should create a group to deal with data collection and forms design in preparation for NIBRS.							X
Revamp forms, procedures, and workflow prior to going to computer-based system.							X
Every 6-12 months, retrain personnel, and evaluate the workflow to correct any bad procedures.							X
The Systems Administrator must understand NIBRS completely.						X	X
Management must be proactive and watch the implementation closely to ensure it stays on track.						X	
"Tweaking" during implementation can cause delays.						X	
Put an experienced full time person in charge of training this should be someone who is computer-literate.					X		
The agency will require sufficient staff if the system is going to work . . . one big cause for failure is not enough of the right kinds of people involved in system implementation and operation.					X		X
The offense report form must be redesigned to have NIBRS-compliant data fields.							X
Some states provide NIBRS error- checking software to the agencies so that the reports sent to the state have fewer errors.					X		

Appendix B: NIBRS Data Elements Analysis

This appendix provides an overview of the NIBRS offense categories and highlights other reference information to assist agencies in ensuring that their data are NIBRS-compliant. The document NIBRS Volume 1: *Data Collection Guidelines*, August 2000, provides detailed information on NIBRS data requirements. [Note: This appendix does not cover every detail of NIBRS data issues. Agencies should refer to *Data Collection Guidelines* for complete coverage of NIBRS data requirements.]

Agencies should contact their state UCR program manager for details on IBR certification and assistance in the proper translation of state penal codes to NIBRS.

B.1 Offenses Reported in NIBRS

There are two categories of offenses reported in NIBRS, Group A and Group B. It is important for the reporting agency to determine to which category an offense belongs because depending on whether a crime is a Group A or B offense the agency should use either a Group A Incident Report or a Group B Arrest Report. The submittal occurs outside the awareness of most users as to what data from Group A or Group B reports will be forwarded to the UCR State Program. Therefore, they should first determine whether their software requires full incident reports on Group B situation(s) before deciding if the distinction is necessary for data entry. Once that distinction has been determined agencies can be aware of the output for their submittals. The Offense Lookup Table, provided in this appendix, will help agencies in mapping offenses to NIBRS crime categories.

B.1.1 Group A Offenses

The following offenses are reported on Group A Incident Reports. There are 22 Group A crime categories consisting of 46 offenses, followed by its UCR Offense Code:

1. Arson (200)
2. Assault Offenses
    - Aggravated Assault (13A)
    - Simple Assault (13B)
    - Intimidation (13C)
3. Bribery (510)
4. Burglary/Breaking and Entering (220)
5. Counterfeiting/Forgery (250)
6. Destruction/Damage/Vandalism of Property (290)

7. Drug/Narcotic Offenses
    - Drug/Narcotic Violations (35A)
    - Drug Equipment Violations (35B)
8. Embezzlement (270)
9. Extortion/Blackmail (210)
10. Fraud Offenses
    - False Pretenses/Swindle/Confidence Game (26A)
    - Credit Card/Automated Teller Machine Fraud (26B)
    - Impersonation (26C)
    - Welfare Fraud (26D)
    - Wire Fraud (26E)
11. Gambling Offenses
    - Betting/Wagering (39A)
    - Operating/Promoting/Assisting Gambling (39B)
    - Gambling Equipment Violations (39C)
    - Sports Tampering (39D)
12. Homicide Offenses
    - Murder and Nonnegligent Manslaughter (09A)
    - Negligent Manslaughter (09B)
    - Justifiable Homicide (09C)
13. Kidnapping/Abduction (100)
14. Larceny/Theft Offenses
    - Pocket-picking (23A)
    - Purse-snatching (23B)
    - Shoplifting (23C)
    - Theft from Building (23D)
    - Theft from Coin-operated Machine or Device (23E)
    - Theft from Motor Vehicle (23F)
    - Theft of Motor Vehicle Parts or Accessories (23G)
    - All Other Larceny (23H)
15. Motor Vehicle Theft (240)
16. Pornography/Obscene Material (370)
17. Prostitution Offenses
    - Prostitution (40A)
    - Assisting or Promoting Prostitution (40B)
18. Robbery (120)
19. Sex Offenses, Forcible
    - Forcible Rape (11A)
    - Forcible Sodomy (11B)
    - Sexual Assault with An Object (11C)
    - Forcible Fondling (11D)
20. Sex Offenses, Nonforcible
    - Incest (36A)
    - Statutory Rape (36B)

21. Stolen Property Offenses (Receiving, etc.) (280)
22. Weapon Law Violations (520)

More information regarding Group A offenses is located in section II, "Offenses" NIBRS Volume 1: *Data Collection Guidelines.*

B.1.2 Group B Offenses

The following offenses are reported on Group B Arrest Reports. They include all offenses that are not Group A offenses, except for most Traffic Offenses. Group B offenses are to be reported using the following 11 crime categories:

1. Bad Checks (90A)
2. Curfew/Loitering/Vagrancy Violations (90B)
3. Disorderly Conduct (90C)
4. Driving Under the Influence (90D)
5. Drunkenness (90E)
6. Family Offenses, Nonviolent (90F)
7. Liquor Law Violations (90G)
8. Peeping Tom (90H)
9. Runaway (90I)
10. Trespass of Real Property (90J)
11. All Other Offenses (90Z)

Required NIBRS data elements and data values are described in detail in *NIBRS Volume 1: Data Collection Guidelines*, August 2000. Data elements are the data fields used in NIBRS to describe the victims, offenders, arrestees, and circumstances of criminal incidents and arrests. Data values are the specific codes that are permitted to be entered into the data elements.

B.2 Offense Lookup Table

Table B.1 lists various types of crime, whether the crime is a Group A or Group B offense, and the NIBRS crime category covering the offense. For example, the crime of Abduction is listed as a Group A offense covered by the crime category Kidnapping/Abduction. The list does not include all of the crimes that can occur; the reporting agency determines whether an unlisted crime is a Group A or B offense.

Agencies should use this table as a guide in mapping their offenses and statutes to NIBRS. The FBI bases its NIBRS offense definitions on common-law definitions. Since most state statutes are also based on common-law definitions, most should fit into the corresponding NIBRS offense classifications, even though details may vary. If a state statute for an offense includes additional offenses not fitting the NIBRS offense definition, the agency should report the nonconforming

offenses according to their NIBRS offense classifications. For example, some states have larceny statutes that are so broadly worded as to include the crime of embezzlement. If embezzlement is perpetrated within such a state, the agency should report the offense to NIBRS as embezzlement, not larceny.

The FBI, Education Training Services Unit can be contacted by phone at 888-827-6427, or by E-mail at ETSU@leo.gov for guidance in developing a state specific conversion table.

Table B.1 Offense Lookup Table

Offense	Group A or B	Corresponding NIBRS Crime Category
–A–		
Abandonment	B	Family Offenses, Nonviolent
Abduction	A	Kidnapping-abduction
Abortion	B	All Other Offenses
Abuse, Nonviolent	B	Family Offenses, Nonviolent or All Other Offenses
Accessory After the Fact	B	(Classify as 90Z if Group A Offense involved or as substantive offense if Group B Offense involved.)
Accessory Before the Fact	B	(Classify as 90Z if Group A Offense involved or as substantive offense if Group B Offense involved.)
Accosting	B	All Other Offenses
Adulterated Food, Drugs, or Cosmetics	B	All Other Offenses (other offenses may have been committed, e.g., Homicide, Aggravated or Simple Assault, or Fraud.)
Adultery	B	All Other Offenses
Affray	B	Disorderly Conduct
Aiding and Abetting	B	(Classify as 90Z if Group A offense involved or as substantive offense if Group B Offense involved.)
Aiding Prisoner to Escape	B	All Other Offenses
Air Piracy-Hijacking	A	(Classify as substantive offense, e.g., Kidnapping-Abduction or Robbery
Alcoholic Beverage Control (ABC) Laws	B	Liquor Law Violations
Antitrust Law Violations	B	All Other Offenses
Arson	A	Arson
Assault	A	Assault Offenses
Assault, Aggravated	A	Assault Offenses
Assault and Battery	A	Assault Offenses
Assault, Minor	A	Assault Offenses
Assault, Sexual	A	(Classify as Forcible Rape, Sodomy, or Fondling; Sexual Assault With An Object; or Statutory Rape.)
Assault, Simple	A	Assault Offenses
Assembly, Unlawful	B	All Other Offenses
Automatic Teller Machine Fraud	A	Fraud Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–B–		
Bad Checks	B	Bad Checks
Battery	A	Assault Offenses
Begging	B	Curfew- Loitering-Vagrancy Violations
Bestiality	B	All Other Offenses
Betting, Unlawful	A	Gambling Offenses
Bigamy	B	All Other Offenses
Blackmail	A	Extortion- Blackmail
Blasphemy	B	Disorderly Conduct
Blue Law Violations	B	All Other Offenses
Boating Law Violations	B	All Other Offenses
Bomb Threat	A	Assault Offenses (Intimidation)
Bombing Offenses	A	(Classify same as substantive offense, e.g., Homicide, Aggravated or Simple Assault, Destruction- Damage-Vandalism of Property, or Weapon Law Violations.)
Bookmaking	A	Gambling Offenses
Breaking and Entering (B&E)	A	Burglary-B&E
Bribery	A	Bribery
Bribery, Sports	A	Gambling Offenses (Sports Tampering)
Buggery (Consenual Sodomy)	B	All Other Offenses
Burglary	A	Burglary-B&E
Burglary Tools, Possessing	B	All Other Offenses
Buying Stolen Property	A	Stolen Property Offenses
–C–		
Canvassing, Illegal	B	All Other Offenses
Card Game, Unlawful	A	Gambling Offenses
Carjacking	A	Robbery
Carrying Concealed Weapon	A	Weapon Law Violations
Checks, Bad	B	Bad Checks
Checks, Fraudulent	B	Bad Checks
Checks, Insufficient Funds	B	Bad Checks

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–C– (Continued)		
Child Abuse, Nonviolent	B	Family Offenses, Nonviolent
Child Abuse, Violent	A	Assault Offenses
Child Cruelty, Nonviolent	B	Family Offenses, Nonviolent
Child Cruelty, Violent	A	Assault Offenses
Child Molesting	A	Sex Offenses, Forcible
Child Neglect	B	Family Offenses, Nonviolent
Civil Rights Violations	B	All Other Offenses (Report predicate offenses, e.g., Arson, Murder, Aggravated Assault.)
Combinations in Restraint of Trade	B	All Other Offenses
Commercialized Sex	A or B	(Classify as Prostitution Offenses, Pornography-Obscene Material, or All Other Offenses.)
Commercialized Vice	A or B	(Classify as Prostitution Offenses, Pornography-Obscene Material, Or All Other Offenses.)
Common Drunkard	B	Drunkenness
Compounding a Felony or Misdemeanor	B	All Other Offenses
Computer Crime	A or B	(Classify same as substantive offense, e.g., Larceny-theft or Embezzlement.)
Concealed Weapon	A	Weapon Law Violations
Conditional Release Violation	B	All Other Offenses
Confidence Game	A	Fraud Offenses
Conflict of Interest	B	All Other Offenses
Consensual Sodomy	B	All Other Offenses
Conservation (Environment or Ecology) Laws	A or B	Destruction-Damage-Vandalism of Property/ All Other Offenses
Conspiracy to Commit	B	(Classify as 90Z if group A Offense involved or as substantive offense if Group B Offense involved.)
Contempt of Court	B	All Other Offenses
Contract Fraud	A	Fraud Offenses
Contributing to the Deliquency of a Minor	B	All Other Offenses (other offenses may have been committed, e.g., Pornography-Obscene Material, Prostitution, or Liquor Law Violations.)
Conversion	A or B	(Classify as Embezzlement, Trespass of Personal Property, etc.)

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–C– (Continued)		
Corrupt Conduct by Juror	B	All Other Offenses (Other offenses may have been committed, e.g., Bribery or False Statement.)
Counterfeiting	A	Counterfeiting-Forgery
Credit Card Fraud	A	Fraud Offenses
Criminal Defamation	B	All Other Offenses
Criminal Libel	B	All Other Offenses
Criminal Slander	B	All Other Offenses
Cruelty to Animal(s)	B	All Other Offenses
Cruelty to Children, Nonviolent	B	Family Offenses, Nonviolent, or All Other Offenses
Cruelty to Children, Violent	A	Assault Offenses
Curfew Violations	B	Curfew-Loitering-Vagrancy Violations
–D–		
Damage Property	A	Destruction-Damage-Vandalism of Property
Deception	A	Fraud Offenses
Defamation, Criminal	B	All Other Offenses
Desecrating the Flag	-	(Not a Criminal Offense)
Desertion	B	Family Offenses, Nonviolent
Destroying Evidence	B	All Other Offenses
Detention, Forcible	A	Kidnapping-Abduction
Detention, Unlawful	A	Kidnapping-Abduction
Dice Game, Unlawful	A	Gambling Offenses
Disinterment, Unlawful	B	All Other Offenses
Disorderly Conduct	B	Disorderly Conduct
Disturbing the Peace	B	Disorderly Conduct
Driving Under the Influence (DUI)	B	Driving Under the Influence
Driving While Intoxicated (DWI)	B	Driving Under the Influence
Drug Equipment Violations	A	Drug-Narcotic Offenses
Drug Offenses	A	Drug-Narcotic Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–D– (Continued)		
Drug Paraphernalia Offenses	A	Drug-Narcotic Offenses
Drunk	B	Drunkenness
Drunk and Disorderly	B	Drunkenness
Drunkard, Common	B	Drunkenness
Drunkard, Habitual	B	Drunkenness
Drunkenness	B	Drunkenness
–E–		
Eavesdropping	B	All Other Offenses
Ecology Law Violations	B	All Other Offenses
Election Law Violations	B	All Other Offenses
Embezzlement	A	Embezzlement
Entry, Forcible	A	Burglary-B&E
Entry, Nonforcible	A	Burglary-B&E
Entry, Unlawful	A	Burglary-B&E
Environment Law Violations	B	All Other Offenses
Equipment, Drug	A	Drug-Narcotic Offenses
Equipment, Gambling	A	Gambling Offenses
Escape (Flight)	B	All Other Offenses
Espionage	B	All Other Offenses (Other offenses may have been committed, e.g., Burglary or Larceny-theft.)
Explosives Offenses	A	(Classify same as substantive offense, e.g., Homicide, Aggravated or Simple Assault, Destruction-Damage-Vandalism of Property, or Weapon Law Violations.)
Extortion	A	Extortion-Blackmail
–F–		
Facilitation of	B	(Classify as 90Z if Group A Offense involved or as substantive offense if Group B Offense involved.)
Failure to Appear	B	All Other Offenses
False Arrest	B	All Other Offenses
False Citizenship	B	All Other Offenses
False Fire Alarm	B	All Other Offenses
False Pretenses	A	Fraud Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–F– (Continued)		
False Report or Statement	A or B	Fraud Offenses
False Report or Statement	B	All Other Offenses
Family Offenses, Nonviolent	B	Family Offenses, Nonviolent
Family Offenses, Violent	A	(Classify same as substantive offense, e.g., Assault Offenses, Homicide Offenses, Forcible Sex Offenses.)
Firearms Violations	A	Weapon Law Violations (Other offenses may have been committed, e.g., Aggravated Assault, Robbery, Disorderly Conduct.)
Fish and Game Law Violations	B	All Other Offenses
Flight to Avoid Confinement, Custody, Giving Testimony, or Prosecution	B	All Other Offenses
Fondling, Forcible	A	Sex Offenses, Forcible
Forcible Dentention	A	Kidnapping-Abduction
Forcible Entry	A	Burglary-B&E
Forcible Rape	A	Sex Offenses, Forcible
Forgery	A	Counterfeiting-Forgery
Fornication (Consensual)	B	All Other Offenses
Fraud	A	Fraud Offenses
Fraud, Automatic Teller Machine (ATM)	A	Fraud Offenses
Fraud, Mail	A	Fraud Offenses
Fraud, Procurement	A	Fraud Offenses
Fraud, Telephone	A	Fraud Offenses
Fraud, Welfare	A	Fraud Offenses
Fraud, Wire	A	Fraud Offenses
Fraudulent Checks	B	Bad Checks
Frequenting a House of Prostitution	B	All Other Offenses
Fugitive	B	All Other Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–G–		
Gambling	A	Gambling Offenses
Gambling Devices Offenses	A	Gambling Offenses
Gambling Equipment Offenses	A	Gambling Offenses
Gambling Goods, Possession of	A	Gambling Offenses
Gambling Paraphernalia, Possession of	A	Gambling Offenses
Gaming Offenses	A	Gambling Offenses
–H–		
Habitual Drunkard	B	Drunkenness
Harassment	B	All Other Offenses
Harboring	B	All Other Offenses
Hate Crime	A or B	(Classify same as substantive offense, e.g., Arson, Assault, Murder, or Destruction-Damage-Vandalism of Property.)
Health and Safety laws (Adulterated Food, Drugs, or Cosmetics)	B	All Other Offenses (Other offenses may have been committed, e.g., Homicide, Aggravated or Simple Assault, or Fraud.)
Hijacking-Air Piracy	A	(Classify as substantive offense, e.g., Kidnapping-Abduction or Robbery.)
Hit and Run (Of a Person)	A or B	Aggravated Assault or Murder if not accidental or All Other Offenses if accidental
Homicide	A	Homicide Offenses
Homicide, Justifiable	A	Homicide Offenses
Homosexual Act or Conduct	B	All Other Offenses
Hostage-Taking	A	Kidnapping-Abduction
House of Prostitution, Frequenting a	B	All Other Offenses
House of Prostitution, Operating a	A	Prostitution Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–I–		
Immigration Law Violations (Illegal Alien Entry, False Citizenship, Smuggling Alien, etc.)	B	All Other Offenses
Impersonation	A	Fraud Offenses
Incendiary Device Offenses	A	(Classify same as substantive offenses committed, e.g., Arson, Homicide, Aggravated or Simple Assault, Weapon Law Violations, or Destruction-Damage-Vandalism of Property.)
Incest	A	Sex Offenses, Nonforcible
Indecent Exposure	B	All Other Offenses
Indecent Liberties	A	Sex Offenses, Forcible (Forcible Fondling)
Influence Peddling	A	Bribery
Insufficient Funds, Checks	B	Bad Checks
Intimidation	A	Assault Offenses
Intoxicated	B	Drunkenness
Intoxication	B	Drunkenness
Invasion of Privacy	B	All Other Offenses
Involuntary Manslaughter	A	Homicide Offenses (Negligent Manslaughter)
–J–		
Joyriding	A	Motor Vehicle Theft
Jury Tampering	B	All Other Offenses (Other offenses may have been committed, e.g., Bribery, Extortion-Blackmail, or Intimidation.)
Justifiable Homicide	A	Homicide Offenses
–K–		
Kickback	A	Bribery
Kidnapping	A	Kidnapping-Abduction
Kidnapping, Parental	A	Kidnapping-Abduction
Killing	A	Homicide Offenses
–L–		
Larceny	A	Larceny-theft Offenses
Libel, Criminal	B	All Other Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–L– (Continued)		
Liquor Law Violations	B	Liquor Law Offenses
Littering	B	All Other Offenses
Loitering	B	Curfew-Loitering-Vagrancy Violations
Looting	A	Burglary or Larceny as appropriate
Lottery, Unlawful	A	Gambling Offenses
–M–		
Mail Fraud	A	Fraud Offenses
Malicious Mischief	A	Destruction-Damage-Vandalism of Property
Mandatory Release Violations	B	All Other Offenses
Manslaughter, Negligent	A	Homicide Offenses
Manslaughter, Nonneglient	A	Homicide Offenses
Manslaughter, Vehicular	A or B	Murder if intentional or All Other Offenses if not intentional
Military Law Violations (AWOL, Desertion, etc.)	B	All Other Offenses
Minor Assault	A	Assault Offenses
Misappropriation	A	Embezzlement
Missing Person	-	(Not a criminal offense)
Molesting, Child	A	Sex Offenses, Forcible
Monopoly in Restraint of Trade	B	All Other Offenses
Moonshining	B	Liquor Law Violations
Motor vehicle Theft	A	Motor Vehicle Theft
Murder	A	Homicide Offenses
–N–		
Narcotic Offenses	A	Drug-Narcotic Offenses
Neglect of Family	B	Family Offenses, Nonviolent
Negligent Manslaughter	A	Homicide Offenses
Nonpayment of Alimony	B	Family Offenses, Nonviolent, or All Other Offenses (if treated as Contempt of Court)
Nonsupport	B	Family Offenses, Nonviolent
Numbers	A	Gambling Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–O–		
Obscene Communication	B	All Other Offenses
Obscene Language, Use of	B	Disorderly Conduct
Obscene Material	A	Pornography-Obscene Material
Obscene Telephone Call	B	All Other Offenses
Obstructing Criminal Investigation	B	All Other Offenses
Obstructing Justice	B	All Other Offenses
Obstructing Police Officer(s)	B	All Other Offenses
Operating a House of Prostitution	A	Prostitution Offenses
–P–		
Pandering	A	Prostitution Offenses
Paraphernalia Offenses, Drug	A	Drug-Narcotic Offenses
Paraphernalia Offenses, Gambling	A	Gambling Offenses
Parental Kidnapping	A	Kidnapping-Abduction
Parole Violation	B	All Other Offenses
Passing Bad Checks	B	Bad Checks
Patronizing a House of Prostitution	B	All Other Offenses
Patronizing a Prostitute	B	All Other Offenses
Peeping Tom	B	Peeping Tom
Perjury	B	All Other Offenses (other offenses may have been committed, e.g., Bribery.)
Perjury, Subornation of	B	All Other Offenses (other offenses may have been committed, e.g., Bribery, Extortion-Blackmail, or Intimidation.)
Pickpocket	A	Larceny-theft Offenses
Pimping	A	Prostitution Offenses
Pocket-Picking	A	Larceny-theft Offenses
Polygamy	B	All Other Offenses
Pornography	A	Pornography-Obscene Material

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–P– (Continued)		
Possession of Burglary Tools	B	All Other Offenses
Possession of Drug Equipment	A	Drug Narcotic Offenses
Possession of Gambling Equipment	A	Gambling Offenses
Possession of Stolen Property	A	Stolen Property Offenses
Privacy, Invasion of	B	All Other Offenses
Probation Violation	B	All Other Offenses
Procurement Fraud	A	Fraud Offenses
Procuring for Prostitution	A	Prostitution Offenses
Profanity	B	Disorderly Conduct
Prostitution	A	Prostitution Offenses
Prostitution, Soliciting for	A	Prostitution Offenses
Prostitution, Transporting Persons for	A	Prostitution Offenses
Prowler	B	All Other Offense
Public Nuisance	B	Disorderly Conduct
Purse-snatching	A	Larceny-theft Offenses
–Q–		
Quarantine, Violation of	B	All Other Offenses
–R–		
Racketeering Influenced and Corrupt Organizations (RICO)	A or B	(Report predicate offenses, e.g., Arson, Aggravated Assault, or Extortion-Blackmail)
Racketeering	A or B	(Classify same as substantive offenses, e.g., Bribery, Extortion-Blackmail, or Larceny-theft Offenses.)
Rape (Forcible)	A	Sex Offenses, Forcible
Rape By Instrumentation	A	Sex Offenses, Forcible
Rape, Statutory	A	Sex Offenses, Nonforcible
Receiving Stolen Property	A	Stolen Property Offenses
Reckless Endangerment	B	All Other Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–R– (Continued)		
Reckless Manslaughter (Nonvehicular)	A	Homicide Offenses (Negligent Manslaughter)
Reckless Operation of Aircraft	B	All Other Offenses
Release Violation, Conditional	B	All Other Offenses
Release Violation, Mandatory	B	All Other Offenses
Resisting Officer	A	Assault Offenses
Restraint, Unlawful	A	Kidnapping-Abduction
Revenue Law Violations	B	All Other Offenses
Riot	B	Curfew-Loitering-Vagrancy Violations (Other offenses may have been committed, e.g., Arson or Destruction-Damage-Vandalism of Property.)
Robbery	A	Robbery
Rout	B	All Other Offenses (Other offenses may have been committed.)
Runaway	B	Runaway (This should be reported though it is not an offense.)
–S–		
Sabotage	B	All Other Offenses (Other offenses may have been committed, e.g., Arson or Destruction-Damage-Vandalism of Property.)
Sanitation Law Violations	B	All Other Offenses
Scalping, Ticket(s)	B	All Other Offenses
Sedition	B	All Other Offenses
Seduction	B	All Other Offenses
Sex, Commercialized	A or B	(Classify as Prostitution Offenses, Pornography-Obscene Material, or All Other Offenses.)
Sex Offenses, Forcible	A	Sex Offenses, Forcible
Sex Offenses, Nonforcible	A	Sex Offenses, Nonforcible
Sexual Assault With An Object	A	Sex Offenses, Forcible
Shoplifting	A	Larceny-theft Offenses
Simple Assault	A	Assault Offenses
Slander, Criminal	B	All Other Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–S– (Continued)		
Smuggling, Alien	B	All Other Offenses
Smuggling, Contraband	B	All Other Offenses (Other offenses may have been committed, e.g., Drug-Narcotic Offenses.)
Sodomy, Consensual	B	All Other Offenses
Sodomy, Forcible	A	Sex Offense, Forcible
Solicitation to Commit Felony	B	(Classify as 90Z if a Group A Offense involved or as substantive offense if Group B Offense is involved.)
Stalking	A	Assault Offenses (Intimidation)
Stolen Property-Buying, Receiving, or Possessing	A	Stolen Property Offenses
Stripping Motor Vehicle	A	Larceny-theft Offenses
Strong-arm Robbery	A	Robbery
Subornation of Perjury	B	All Other Offenses (Other offenses may have been committed, e.g., Bribery, Extortion-Blackmail, or Intimidation.)
Suicide	-	(Not a criminal offense)
Suspicion	-	(Not a criminal offense)
Swindle	A	Fraud Offenses
–T–		
Tax Law Violations	B	All Other Offenses
Telephone Call, Threatening	A	Assault Offenses (Intimidation)
Telephone Fraud	A	Fraud Offenses
Terrorism	A	(Classify same as substantive offense, e.g., Assault, Destruction-Damage-Vandalism of Property, or Murder.)
Theft	A	Larceny-theft Offenses
Theft From Building	A	Larceny-theft Offenses
Theft From Coin-Operated Machine or Device	A	Larceny-theft Offenses
Theft From Motor Vehicle	A	Larceny-theft Offenses
Theft of Motor Vehicle Parts or Accessories	A	Larceny-theft Offenses
Theft of Vehicles or Equipment Other than Motor Vehicles	A	Larceny-theft Offenses

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–T– (Continued)		
Threatening Behavior	A	Assault Offenses (Intimidation)
Threatening Conduct	A	Assault Offenses (Intimidation)
Threatening Gesture	A	Assault Offenses (Intimidation)
Threatening Telephone Call	A	Assault Offenses (Intimidation)
Threatening Words or Statement	A	Assault Offenses (Intimidation)
Threats	A	Assault Offenses (Intimidation)
Traffic Violations	B	Do not report except for Driving Under the Influence (DUI), Driving While Intoxicated (DWI), Hit and Run, or Vehicular Manslaughter.
Transmitting Wagering Information	A	Gambling Offenses
Transporting Persons for Prostitution	A	Prostitution Offenses
Treason	B	All Other Offenses (Other offenses may have been committed, e.g., Burglary or Larceny.)
Trespass of Personal Property	B	All Other Offenses
Trespass of Real Property	B	Trespass of Real Property
–U–		
Unauthorized Use of a Motor Vehicle (no lawful access)	A	Motor Vehicle Theft
Unauthorized Use of a Motor Vehicle	A or B	Embezzlement (lawful access but the entrusted vehicle is misappropiated) or All Other Offenses (the unlawful taking of a vehicle for tempory use when prior authority had been granted or can be assumed, such as in family situations; a complaint is filed and an arrest made)
Unlawful Assembly	B	Curfew-Loitering-Vagrancy Violations
Unlawful Entry	A	Burglary-B&E
Unlawful Restraint	A	Kidnapping-Abduction
Unlicensed Weapon	A	Weapon Law Violations
Unregistered Weapon	A	Weapon Law Violations
Uttering Bad Checks	B	Bad Checks

Lookup Table (Continued) Offense	Group A or B	Corresponding NIBRS Crime Category
–V–		
Vagabondage	B	Curfew-Loitering-Vagrancy Violations
Vagrancy	B	Curfew- Loitering-Vagrancy Violations
Vandalism	A	Destruction-Damage-Vandalism of Property
Vehicular Manslaughter	A or B	Murder and Nonnegligent Manslaughter (if not accidental) or All Other Offenses (if accidental)
Vice, Commercialized	A or B	(Classify as Prostitution Offenses, Pornography-Obscene Material, or All Other Offenses.)
Violation of Quarantine	B	All Other Offenses
Violation of Restraining Order	B	All Other Offenses
–W–		
Wagering, Unlawful	A	Gambling Offenses
Weapon, Concealed	A	Weapon Law Violations
Weapon, Unlicensed	A	Weapon Law Violations
Weapon, Unregistered	A	Weapon Law Violations
Weapon Law Violations	A	Weapon Law Violations
Welfare Fraud	A	Fraud Offenses
Wire Fraud	A	Fraud Offenses
Wiretapping, Illegal	B	All Other Offenses

B.3 Quality Control

Ensuring the highest quality of data is crucial at each step in the crime reporting system: from the officer entering the incident-based report, to the local RMS, to the state program, and up to the national system. In an effort to ensure the accuracy of data in the national Uniform Crime Reporting Program (UCR) database, the staff consistently review all submissions for discrepancies. A list of those NIBRS incidents which are questionable are sent to the UCR Program Managers for their attention. All adjustments must be made electronically in order for the national database to be updated. The following are examples of some of the most common discrepancies found in the NIBRS incidents submitted:

1. Burglary (offense code 220) and Larceny-theft (offense codes 23 A-H) reported in the same incident. (See Volume 1: *Data Collection Guidelines,* p. 24.) "For NIBRS purposes, Larceny-theft is an element of Burglary. . . ."

2. Data Element 15, Property Description 01 = Aircraft is being reported as property stolen. (See Volume 1: *Data Collection Guidelines,* p. 83.)

3. Data Element 15, Property Description 29 = Structures–Single Occupancy Dwelling, 30 = Structures–Other Dwellings, 31 = Structures–Other Commercial/Business, 32 = Structures–Industrial/Manufacturing, 33 = Structures–Public/Community, etc. These are reported as the property taken in Larceny-theft all other (23H). (See Volume 1: *Data Collection Guidelines,* p. 84.)

4. Aggravated assaults (offense code13A) with no weapon and no injuries reported. (See Volume 1: *Data Collection Guidelines,* pp. 22-23.)

5. Simple assaults (offense code 13B) with injuries (minor) and no weapons. (See Volume 1: *Data Collection Guidelines,* p. 23.)

6. Arson (offense code 200) using Property Description 15, 77 = Other with high dollar values as burned reported. (See Volume 1: *Data Collection Guidelines,* p. 85.)

7. Negligent Manslaughter (offense code 09B) being reported and are seeing the weapon reported as vehicle and offender suspected of using, Data Element 8, using alcohol and drugs (A, D). The possibility of Driving Under the Influence (DUI) deaths being reporting under 09B offense code is being questioned. (See Volume 1: *Data Collection Guidelines,* p. 29.)

8. Incest (offense code 36A) using wrong relationship codes, Data Element 35, i.e., (FR, AQ, OK, BG, etc.). (See Volume 1: *Data Collection Guidelines,* pp. 97-98.)

9. Incest (offense code 36A) and Statutory Rape (offense code 36B) seeing ages of victims 8 years and under in frequent amounts. Should consider forcible rape because a person 4 years of age does not have the mental capacity for consensual sex. (See Volume 1: *Data Collection Guidelines,* pp. 33-34.)

10. Data Element 3, Incident Date/Hour (00) used often in many incidents for NIBRS. This indicates the offense occurred on or between midnight and 0059. If the incident hour is unknown, the hour should be left blank. (See Volume 1: *Data Collection Guidelines,* p. 69.)

11. Data Element 13, Type Weapon/Force Involved, 40 = Personal Weapons is often indicated in forcible sex offenses. The definition infers that some force is going to be used during the commission of the offense. Submitting personal weapons as being used in every forcible sex offense should not be automatic, especially in cases where the victim succumbs to the offender out of fear. However, weapons should be indicated when the victim sustains minor injuries, or wherein the offender uses a weapon or displays it in a threatening manner, or the victim suffers obvious severe or aggravated bodily injury involving apparent broken bones, loss of teeth, possible internal injury, severe laceration, or loss of consciousness. (See Volume 1: *Data Collection Guidelines,* pp. 80-81.)

12. Shoplifting (offense code 23C) with Data Element 25, I = Individual as the victim. The majority of these incidents should indicate that B = Business is the victim.

13. Some NIBRS data indicates a broad range for victim/offender ages, Data Element 26. Example is 01-99 as the victim/offender age reported in a particular incident. The national Program will indicate the middle of the range, (49). It is important to narrow the range of age one of reason, i.e., 25-35. (See Volume 1: *Data Collection Guidelines,* pp. 91-92.)

14. Data Element 35, Relationship(s) of Victim to Offender(s). Some of the data indicates a 10 year old being a parent.

15. Data Element 15, Property Description 99 = (blank). This is a special category to be used by the national UCR Program to compile statistics on certain designated types of property, e.g., cellular phones, which are the object of theft fads. Currently this is not used by the national UCR Program. Some NIBRS data contains this very code which is not currently being used. (See Volume 1: *Data Collection Guidelines,* p. 85.)

16. Data Element 26 Age (of Victim). Some data indicates a 99 year old as the victim. In NIBRS 99 = Over 98 Years Old; 00 = Unknown.

17. In incidents of Theft of Motor Vehicle Parts or Accessories (23G), Data Element 15 contains Property Description 26 = Radios/TVs/VCRs in many instances. In all probability this should be Property Description 38 = Vehicle Parts/Accessories.

18. Offender Sequence Numbers of 01, 02, etc., with unknown offender age, sex, and race information in Data Elements 37, 38, and 39; this could very well be the case if someone is knocked to the ground and knows only that two suspects perpetrated a crime; however, the national Program review indicates a high volume of incidents which contain offender sequence numbers with unknown information. If there is some descriptive information observed by the victim with respect to any of the sequenced offenders please indicate, i.e., male, female, white, black, etc. Offender Segments are used to describe the offenders in the incident (e.g., their age, sex, and race). An Offender Segment should be submitted for each of the (up to 99) offenders involved in the incident. There must be at least one Offender Segment in each incident report. (See Volume 1: *Data Collection Guidelines,* p. 63.)

19. Estimated Drug Quantity, Data Element 21. (See Volume 1: *Data Collection Guidelines,* p. 89.) "This data element should be used to indicate the quantity of drugs or narcotics seized in a drug case. Therefore, it should be used only if one of the offenses in the incident was 35A Drug/Narcotic Violations, 6 = Seized was entered into Data Element 14 (Type Property Loss/Etc.), and 10 = Drugs/Narcotics was entered into Data Element 15 (Property Description). If the substance was sent to a laboratory for analysis, and response has not yet been received, then 1 = None must be entered into Data Element 21 to indicate None. This is an interim report and should be later updated with the true quantity." It is apparent the updating of these incidents is not occurring because the computer generated "year-end report" indicates an unusually high amount of 1 = None, remaining in the database.

20. In many offenses of Credit Card/Automatic Teller Machine Fraud (26B) the national Program is becoming aware of agencies indicating credit/debit cards (09) in Data Element 15 (Property Description) as stolen property reported for this specific offense. The credit/debit card may have been previously stolen, however, the property which was purchased with the stolen credit card should be listed in Data Element 15. According to the *Uniform Crime Reporting Handbook,* NIBRS Edition, page 16, Credit Card/Automatic Teller Machine Fraud is defined as "The unlawful use of a credit (or debit) card or automatic teller machine for fraudulent purposes." This offense does not apply to the theft of a credit/debit card but rather its fraudulent use.

21. It has come to the attention of the national Program that the offense of Robbery (120), data received from law enforcement indicates several robbery incidents with only a business as the victim in Data Element 25 (Type of Victim). According to the NIBRS Volume 1: *Data Collection Guidelines,* page 33, "The victims of a robbery include not only those persons and other entities (businesses, financial institutions, etc.) from whom property was taken (or was attempted to be taken), but also those persons toward whom the robber(s) directed force or threat of force in perpetrating the offense. Therefore, although the primary victim in a bank robbery would be the Financial Institution, the teller toward whom the robber pointed a gun and made a demand should also be reported as a victim."

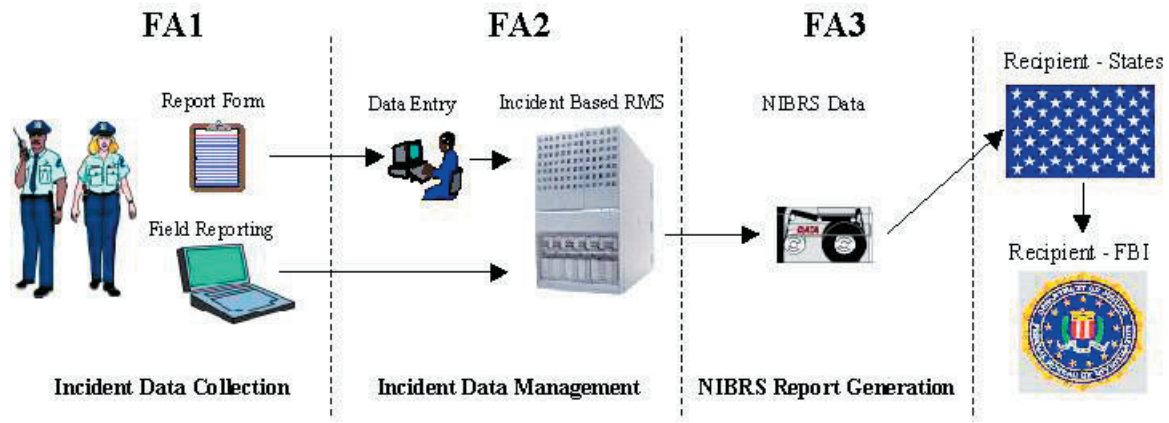
Appendix C: Cost Model User Information

This appendix provides additional detail on the cost model. In section C.1, the structure of the model is presented. Section C.2 describes the assumptions used to develop each of spreadsheets in the model. Section C.3 provides a cost model user guide, which focuses on three important sheets: the *Introductory Screen*; *External Inputs*; and *Cost Report*. A simplified, one page user instruction guide is also included in section 3. Variables used in the model are listed in section C.4. Although one does not have to know each value in order to use the model, the list helps to trace the interaction of variables if so desired.

C.1 Cost Model Structure

The cost model encompasses only those components necessary to enable law enforcement agencies to collect and submit NIBRS data to state and federal authorities. The allocation of costs generated by this model can, therefore, be completely attributed to NIBRS if the sole purpose of procuring the system is to participate in NIBRS. Since many agencies make the decision for a new RMS based on multiple factors and not a NIBRS upgrade alone, it is difficult to segregate the NIBRS costs unless the agency is upgrading with the same vendor and only adding NIBRS in the upgrade. It is possible in this situation, and in others, that there may be no added costs for the NIBRS capability. [As depicted in Figure C.1, each successive functional area (FA), "FA1—Incident Data Collection" and "FA2—Incident Data Management," must exist in order to proceed ultimately to "FA3—NIBRS Report Generation."] Therefore, in order to perform FA3, the agency must first have FA1 and FA2 in place. The cost model elements associated with each functional area are described in Figure C.1.

Figure C.1 Functional Area Progression



Functional Area 1—Incident Data Collection

The cost model addresses the following costs associated with the functional area of incident data collection:

- **Train Officers.** Train officers to obtain the necessary incident-level data at the crime scene. At a minimum, this training would include the 53 elements of NIBRS.
- **Procure a Field Reporting System (Optional).** Field reporting (using MDCs to enter incident data directly into the RMS or to upload these data at a later time) is included in order to enable agencies to streamline their data collection process. Even though many agencies use this component, others have successful NIBRS-compliant RMSs without computerized field reporting.

Functional Area 2—Incident Data Management

The following elements within the cost model address:

- **Procure an Incident-based RMS.** The agency should purchase the software, hardware, and installation services necessary to implement a new incident-based RMS, or upgrade an existing non-incident-based RMS to incident-based capabilities. Information obtained through interviews with COTS RMS vendors and agencies developing custom RMSs indicated that the ability to generate NIBRS reports was a built-in feature of a new or upgraded incident-based RMS. Therefore, this report-generating feature would not have to be procured separately at the time of the purchase or at a later date.
- **Procure an Information Technology Infrastructure.** The agency should obtain all workstations, printers, LAN, WAN, and telecommunications components necessary to facilitate data exchange with the incident-based RMS.
- **Annual Recurring Costs.** The agency should pay for annual renewal of software and hardware maintenance services and annual telecommunications expenses (i.e., circuit access and user network interface [UNI] charges).
- **Train Data Entry Personnel.** The agency should train data entry personnel to properly enter incident data, including such processes as entering incident data from written report forms or from dictated notes. If mobile data entry/field reporting occurs there is still a critical role for data entry staff to maintain data quality. Offense classifications and other critical data are best reviewed after reports are electronically transferred to the agency by staff trained and experienced in the NIBRS classification system to assure data credibility.
- **Train System Administrators.** The agency should train personnel for system administration functions.

Functional Area 3—NIBRS Report Generaion

The last functional area covered by this cost model is NIBRS report generation, which is necessary for the submission of NIBRS data to state and federal authorities.

Procure NIBRS Reporting Capability. As stated previously, this ability is a built-in feature of new incident-based RMSs and of those RMSs that have been upgraded to incident-based capability. Agencies that operate older incident-based RMSs without NIBRS reporting capabilities must procure this feature as a COTS add-on module from a vendor or have the module custom developed for their system.

C.2 Assumption in the Cost Sheets

The following are brief overviews of the Cost Sheets that are the heart of the model. Each sheet is a Microsoft Excel™ spreadsheet that is linked to the User Interface, Internal Parameters, and Model Output sheets. More detailed descriptions of each Cost Sheet are contained in the Excel cost model and in the cost model documentation.

The primary input for many of the cost sheets is the number of concurrent users for the NIBRS capable RMS. The number is based on the number of incidents an agency reports per month and the number of sworn officers it has. The number of incidents per month determines the number of data entry clerks that would be required to process the information. The number of sworn officers determines the number of concurrent query users as explained below.

C.2.1 Data Entry Users

The number of data entry users is based on the business model where sworn officers record the incident information on paper and data entry operators enter the data from the paper form. Results from agency interviews performed during this study indicated that this business model was the one that was most frequently used.

The model assumes that each data entry operator averages seven full production hours per day, works 22 days per month, and enters nine[2] incidents per hour. This results in each data entry operator entering 1,386 incidents per month. Thus, if an agency has 4,800 incidents per month, it would use four data entry operators.

[2]The rate of *nine per hour* is based on data provided through agency interviews.

C.2.2 Query Users

The number of query users is based on the business model where detectives are the primary query users. A statistical analysis of agency data demonstrated that approximately 15% of sworn officers are detectives. Interviews conducted for this study determined that approximately 25% of detectives might be involved in data analysis during the day. Thus, by multiplying 15% by 25%, the percent of sworn officers performing queries at any time is approximately 3.75%, which was rounded to 5%.

A concurrent user escalation factor of 10% of the total of data entry and query users was added to ensure that actual concurrent users do not exceed the calculated number (i.e., additional concurrent users not specifically addressed in this model could be crime analysts, chiefs, supervisors, and other non-data entry or investigative individuals).

C.2.3 NIBRS Software

The NIBRS software cost element includes the purchase costs of acquiring the custom or COTS software an agency requires implementing the NIBRS-compliant RMS. The costs associated with installing the software are included separately under Installation Costs. The model allows the user to choose either custom-developed or COTS systems.

The processes for estimating RMS costs are described in the following two sections.

C.2.3.1 Custom-Developed System

This section describes the method used to estimate the customized system development effort of a core RMS compatible with the NIBRS requirements. The model addressees three scenarios that include: no RMS, RMS without IBR functionality, and RMS with IBR functionality but not NIBRS compliant. The level of effort for an agency to go from the initial state to fully compliant differs with each of the three scenarios. Analysis of the data model for NIBRS determined the number of function points that would be required to be implemented through code development in order for an agency to achieve NIBRS capability.

Function Point Analysis is a method for sizing software projects based upon the number of data elements and user interaction with the system. The advantage of the function point approach is that it bases the size of the application on characteristics that are not based on the programming language used. A function point consists of the weighted total of five external aspects of software applications, including:

- Types of *inputs* to the application, such as data entry screens.
- Types of *outputs* that leave the application, such as reports.
- Types of *inquiries* or *queries* that users can make in the system.
- Type of *logical* or *internal files* that the application maintains, such as data tables.
- Type of *interfaces* to other applications or *external files* that the system requires, such as reference files like Master Name Index table.

The resulting number of function points for each scenario was entered into the KnowledgePLAN[3] software cost-estimating model that was developed by Capers Jones. The model incorporates the experience of nearly 7,000 software development projects and provides estimates of the number of staff months of effort required for system development based on the number of function points. The estimated number of staff months includes the efforts for system design, development, testing and installation.

C.2.3.2 Field Reporting

The model has the capability to include the costs of field reporting. The model asks the user for the number of concurrent mobile users and then applies a per-laptop cost and the price of one server license. These costs apply only to agencies that are using COTS applications for their RMS. It is assumed that any custom-development effort would include this capability and there would be no additional license costs.

The cost model does not include any costs for radio transmission of information from the laptops to the RMS server. The model assumes that uploads take place through the use of floppy disks for information transfer. The costs associated with field reporting go beyond the costs that are required to implement the NIBRS-RMS. The cost of this capability is included for agencies that are considering acquiring field reporting in addition to NIBRS.

C.2.4 Database Software

The Database Software Cost element includes the purchase costs of acquiring the software licenses needed (for servers and concurrent users) to implement the NIBRS-compliant RMS in an agency. The costs associated with installation are included in Installation Costs.

[3] KnowledgePLAN is a product of Software Productivity Research.

C.2.5 Hardware

The Hardware Cost element includes the purchase costs of acquiring the additional hardware needed to implement the NIBRS-compliant RMS in an agency. The costs for the workstations, servers, and laptops, hubs, and printers are also included. However, the costs associated with installation are not included in this cost element.

C.2.6 Training

Training refers to the one-time training services needed to facilitate instruction and through which operations personnel acquire sufficient skills to operate or maintain a NIBRS-compliant RMS with maximum efficiency. This cost element includes the cost of training the necessary personnel, but does not include costs of travel associated with their training.

C.2.6.1 Train the Trainers

Law enforcement agency trainers will receive three days of training in order to prepare them to train the agency's NIBRS-RMS users. The cost model uses a class size of 10 students. Small agencies will have fewer personnel to train. The model assumes one trainer will receive three days of vendor-supplied training and that this trainer would attend a class that would include trainers from more than one agency, and therefore, the costs would be a per seat basis.

C.2.6.2 End-user Training

One class, or 10 trained trainers, would be sufficient to handle the training needs of medium and large agencies. Interviews with some agencies indicate that end-user training is normally accomplished at regular in-service training. For these agencies, training did not exceed their usual in-service training budget. Other agencies experienced an additional cost. Because the costs are so variable the model does not attribute any additional costs to end-user training. Larger agencies might want to add end-user training costs to the figure produced by the cost model. For a benchmark, some agencies recommend three days of training every six months.

C.2.6.3 System Administrator Training

There is no system administration training for stand-alone systems. Administrators with agencies that have LANs will receive two days of training; large agencies with WANs will receive five days of training. Vendors indicated that at least one week is required for administrator training for large installations. Vendors also indicated that one class of 10 administrators should be sufficient for large agencies; medium agencies usually require three to four administrators, one for each shift.

C.2.7 System Installation

The system installation cost element includes the costs associated with designing, planning, and installing the system and the system certification. Installation costs for software, hardware, and circuits are provided in the following three subsections.

C.2.7.1 Software Installation

Installation procedures vary as systems range in size from single location stand-alone to multi-location (districts or precincts) in a large networked agency. The smaller systems can usually be installed in one day. Installation of medium-sized systems appears to require one week, and installation of the large systems can require up to two weeks.

The cost model assigns one day for installation at small agencies, five days for medium, and ten days for large agencies.

C.2.7.2 Hardware Installation

The hardware installation cost element covers the costs of installing wall ports and cabling required for the network installation of the server, routers, and the additional workstations, and printers. The model computes the costs associated with the number of additional workstations and printers that are entered through the initial user interface.

C.2.7.3 Circuit Installation

The circuit installation covers the cost of installing the transport circuit that will connect the site to the service provider's Point of Presence (POP) and the cost of the UNI. Circuit installation costs vary depending on the committed information rate chosen (64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, 768 Kbps or 1024 Kbps). These costs were obtained through the GSA's FTS2001 Year 1 contract.

C.2.8 Data Conversion

The data conversion cost element includes the initial costs incurred in migrating data from legacy RMSs to the newly installed incident-based RMS. This cost element is limited to the cost of converting the Master Name Index.

The legacy data structure must be examined and then mapped to the new data structure contained in the RMS. Once the structures have been mapped, conversion code is written and the legacy data converted to the new data structure.

Data conversion prices do not include efforts to improve the quality of the legacy data by examining it to remove errors that were caused through data entry.

The model assumes that there will be no data conversion costs for a small agency with no RMS since it does not have a legacy system from which to convert. The conversion costs estimates do not include any costs for manually re-keying the paper reports. This is an area of high uncertainty for an agency because the conversion costs could be significantly higher depending on the quality of the legacy data.

C.2.9 Software Maintenance

Software maintenance involves ensuring the continued reliability of the system and its underlining components, updating the capabilities of the off-the-shelf components (e.g., by installing new software versions that contain any corrections and updates), and providing help desk support to the users.

Help desk support is normally provided for 8 hours per day, 5 days per week, (8 x 5), or around-the-clock (24 x 7). Vendors and agencies report that 8 x 5 coverage was 15% of the cost of the RMS licenses and 24 x 7 coverage ranged from 25% to 30%.

There are no annual maintenance costs for the database licenses.

C.2.10 Hardware Maintenance

Hardware maintenance includes maintenance, preventive, remedial diagnostic and repair services. It can also include field-engineering change or field modification to equipment (custom solutions). Maintenance services are preventive actions that enable the hardware to continue to operate as designed. Repair services are corrective actions that restore the item to normal operating condition following an interruption or breakdown.

The Gartner Group provided industry cost factors for hardware maintenance beyond the initial warranty period. Gartner indicated that the normal industry practice was a cost of 10% of the purchase price for 8 x 5 support and 17.5% for 24 x 7 support.

New computer hardware normally has a one- to three-year warranty period included in the purchase price. The hardware maintenance costs computed by the cost model are for equipment beyond their initial warranty period.

C.2.11 Annual Telecommunications

Annual telecommunications costs include:

- Circuit access.
- UNI.
- Transport.
- Port (located at the Point of Presence).

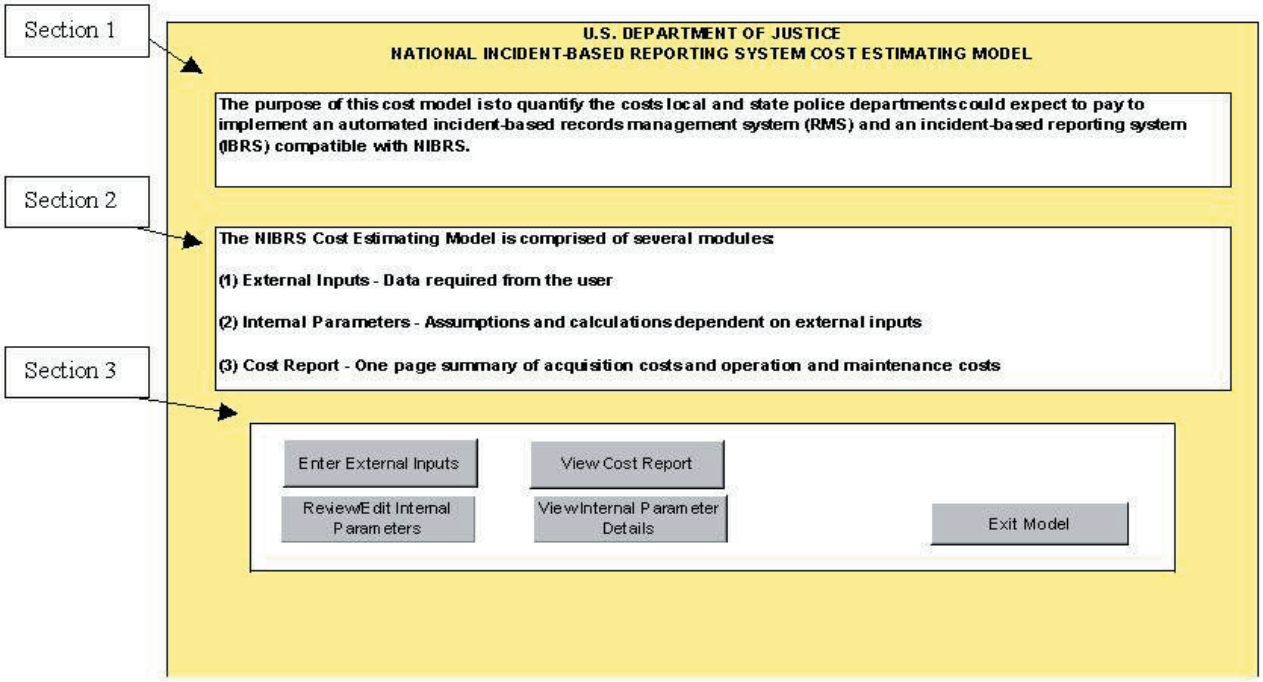
These costs vary depending on the committed information rate chosen and were obtained through the GSA's FTS2001 Year 1 contract.

C.3 Cost Model User Guide

C.3.1 Introductory Screen

The introductory screen for the NIBRS-RMS Cost Estimating Model is composed of three sections (see Figure C.2). Section 1 contains a brief description of the purpose of the model. Section 2 highlights the three main modules in the model. Section 3 contains macro-driven push buttons that will assist the user in navigating the model.

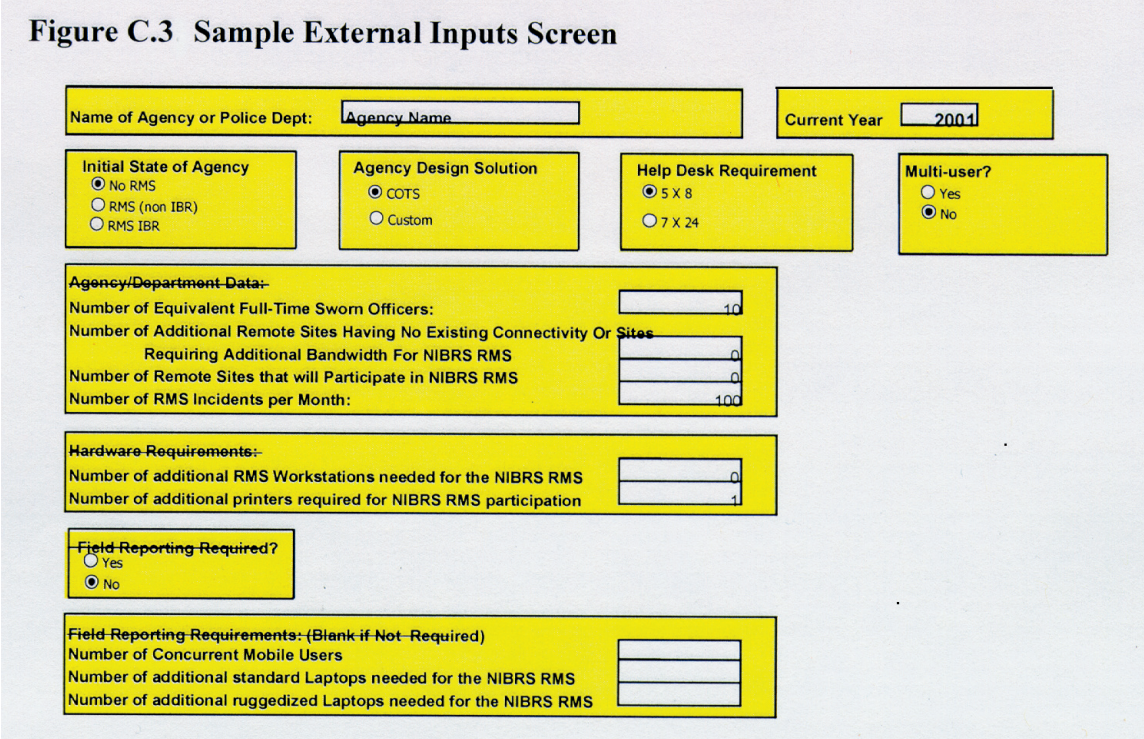
Figure C.2 Introductory Screen



Explanation of Section 3

- "Enter External Inputs" transfers the user directly to the external input sheet (see Figure C.3).
- "View Cost Report" takes the user directly to the output report screen (see Figure C.4).
- "Review/Edit Internal Parameters" allows the user to view the values used in the model's calculations. These internal parameter values are password protected and may only be changed by authorized personnel.
- "View Internal Parameter Details" transfers the user to a menu containing push buttons for the cost categories presented in the model. By selecting a cost category, the user can review a detailed sheet listing the assumptions, data sources, variables, formulas, and calculations underlying the model.
- "Exit Model" closes the model. If changes have been made, the user will be asked if the changes should be saved. Clicking on "yes" saves the changes under the current file name. To save under a different file name, click on "File" on the Excel™ tool bar, choose "Save As" and enter the desired file name at the prompt.

Figure C.3 Sample External Inputs Screen



Explanation of External Inputs Screen as Shown in Figure C.3

- On the External Inputs Screen, the user first inputs the name of the agency and then the current year.
- Next, by clicking on the appropriate buttons the user provides required information about the initial state of the agency, the agency's design solution, the agency's help desk requirements, and whether the system will be a multi-user system.
- The user then must enter information about the agency/department. This information includes the number of full-time equivalent sworn officers, the number of additional sites having no connectivity or requiring additional bandwidth, the number of remote sites, and the number of RMS incidents per month. Information for these questions is entered in the white boxes.
- The user next provides the hardware requirements, which include the number of additional RMS workstations and printers required for NIBRS RMS participation.
- The user indicates whether the agency/department requires field reporting. If "Yes," then the user must provide the field reporting requirements, which include the number of concurrent mobile users and the number of additional standard or ruggedized laptops required for a NIBRS capable RMS. If the user answers "No," no further information is required. (Note: If field reporting data is present from a previous estimate but the user does not want field reporting for a new estimate, the number of concurrent users and laptops must be re-entered as zero.)

- The push buttons located at the top of the external input screen are the same as on the introductory screen with the exception of "Return to Introduction" and "Print Inputs." "Print Inputs" will print the current external input screen only.

Figure C.4 Sample Cost Report Screen

Agency/Department:	Agency Name		
Initial Investment Cost Category	Initial Investment	System O& M Cost Category	Annual Operations & Maintenance Costs
Hardware		Hardware Maintenance	$ 308
RMS Server & Accessories	$ 2,679	Software Maintenance	$ 450
User Equipment	$ 400	Telecommunications	$ -
Software			
RMS	$ 3,000		
Database Licenses	$ 1,521		
Training	$ 598		
Installation	$ 1,061		
Data Conversion	$ -		
Total Initial Costs	$ 9,259	Annual O & M Costs	$ 758
Initial State:	No RMS	Help Desk:	5 X 8
Solution:	COTS	Multi-user?	No
Number of Equivalent Full-Time Sworn Officers:			10
Number of Additional Remote Sites Having No Existing Connectivity or Sites Requiring Additional Bandwidth for NIBRS RMS:			0
Number of Remote Sites that will Participate in NIBRS RMS:			0
Number of RMS Incidents per Month:			100
Number of additional RMS Workstations needed for the NIBRS RMS:			0
Number of additional printers required for NIBRS RMS participation:			1
Field Reporting Required?			No
Number of Concurrent Mobile Users:			0
Number of additional standard Laptops needed for the NIBRS RMS:			0
Number of additional ruggedized Laptops needed for the NIBRS RMS:			0

Explanation of View Cost Report Screen As Shown in Figure C.4

When "View Cost Report" is selected, the user is transferred to the report screen shown in Figure C.4. This report contains the total initial investment costs and the annual cost for the operation and maintenance of the system. By clicking on the question marks next to the RMS Server & Accessories and User Equipment cost categories, the user will be able to view a more detailed cost breakout for these items.

The push buttons on the cost report sheet are located on the right-hand side of the report. To change any of the external inputs, the user must return to the "Enter External Inputs" screen. Changes cannot be made on the cost report screen.

The upper section of the output lists the costs that have been calculated by each of the appropriate Cost Sheets. The bottom half of the sheet contains a listing of the external parameters that have been supplied by the user. The user will not be able to change the values in the internal parameter section of the Model Output. By going back to the External Inputs button and changing the value of one of the external parameters, the user can see the changes in costs resulting from changes in the external parameters. Instructions for completing a simplified cost model are provided on the next page.

Simplified Cost Model User Instructions

Step One:
Open the Excel™ file containing the cost model.

Step Two:
A box will appear with the following options:

- *Disable Macros*
- *Enable Macros*
- *More Info*

Single click on the *Enable Macros* button.

Step Three:
A box will appear with the following options:

- *To update all linked information, click Yes*
- *To keep the existing information, click No*

Single click on the *No* button.

Step Four:
Read the Introduction screen that appears. Single click on the *Enter External Inputs* button to begin entering agency specific parameters.

Step Five:
Enter agency specific parameters. Any parameters with zero values for your agency may be left blank. For boxes with circles next to the options, point and click on the appropriate option for your agency.

There are buttons across the top of the screen to help you move around the model. To view the values of the internal parameters, which are not agency specific, single click on the *Review Input and Parameters* button. This data are protected and cannot be changed.

Step Six:
Single click on the *Return to External Inputs* button. If satisfied with the input, single click on the *View Cost Report* button, which will allow you to view the projected cost of NIBRS-RMS implementation for your agency.

Step Seven (optional):
Single click on the *Return to Introduction* button. Explore the underlying sheets in the model by single clicking on the *View Internal Parameters Detail* button. Another sheet with various buttons will appear that will allow you to examine Initial Investments/Acquisition Details sheets and O&M Details sheets.

Step Eight:
Single click on the *Exit Model* button when finished. It is recommended that you use the Excel™ File - Save As option if you wish to save each scenario you create under a different name.

C.4 Cost Model Variables

Many variables are referenced in numerous places throughout the cost model. Table C.1 summarizes the variable names and tables used in the cost model as well as their original input location. Table C.1 also provides the spreadsheet in which the value of each variable is originally defined. The user can make original definitions by entering a numerical value for the variable or by calculating the value of the variable as a function of previously defined variables. Table C.2 summarizes the list of look-up tables used in the cost model. The purpose of providing Tables C.1 and C.2 is to simplify the process of making changes to the driving variables of the model and to ensure that variables are changed only at their original output location.

Table C.1 NIBRS Cost Estimating Model

Variable Name	Definition	Original Input Location	Worksheets Where Used
C_USERS	Number of concurrent users	Assumptions	Users NIBRS SW DB SW Hardware
Q_DE	Number of data entry clerks	Assumptions	Users
Q_QUERY	Number of personnel using the system for queries at any one time	Assumptions	Users
Q_DAYS	Average number of working days per month	Internal	Users
Q_HOURS	Average number of working hours per month	Internal	Users
I_HOURS	Average number of incidents per hour by a data entry clerk	Internal	Users
PERCENT _ SO	Percent of sworn officers making concurrent queries	Internal	Users
PERCENT_CUSER	Concurrent user escalation factor (percent)	Internal	Users Assumptions
SW	Total purchase price of software	NIBRS SW	SW Maint NIBRS SW
SW_COTS	Cost of COTS software license	NIBRS SW	NIBRS SW
SW_CUSTOM	Cost of custom software development	NIBRS SW	NIBRS SW

Cost Model (Cont'd) Variable Name	Definition	Original Input Location	Worksheets Where Used
SM	Staff months needed to develop custom software	NIBRS SW	NIBRS SW
UC_SM	Unit cost of a staff month	Internal	NIBRS SW
UC_L_1	Cost of 1 month of NIBRS SW license	Internal	NIBRS SW
UC_L_10	Cost of 10 NIBRS SW license	Internal	NIBRS SW
UC_L_100	Cost of 100 NIBRS SW license	Internal	NIBRS SW
UC_FIELD_SER	Unit cost of a field mobile server license	Internal	NIBRS SW
UC_FIELD_USER	Unit cost of laptop license	Internal	NIBRS SW
Q_MOBILE	The number of mobile users	RMS	NIBRS SW
FIELD_RPT	Field reporting requirement (Yes or No)	RMS	NIBRS SW
DBSW	Total purchase price of database software licenses	DB SW	DB SW
UC_DATABASE	Base cost of software license	Internal	DB SW
UC_DBSWUSER	Cost of additional concurrent user licenses (after first five)	Internal	DB SW
UC_SER1	Unit cost of a stand-alone RMS server	Internal	Hardware
UC_WKS	Unit cost of a high-end desktop PC (includes Windows NT operating system, network card, and monitor)	Internal	Tables Hardware
UC_LAP	Unit cost of a mid-level notebook with active matrix screen	Internal	Tables Hardware
UC_LAPR	Unit cost of a ruggedized laptop	Internal	Tables Hardware
UC_ROUTER	Unit cost of a router for the headquarters or a remote site	Internal	Tables Hardware
UC_PTR	Unit cost of the average stand-alone printer	Internal	Tables Hardware
UC_PTRN	Unit cost of the average stand-alone networked printer	Internal	Hardware

Cost Model (Cont'd) Variable Name	Definition	Original Input Location	Worksheets Where Used
UC_HUB	Unit cost of the average network hub port	Internal	Tables Hardware
TRAIN	Total program cost of training	Training	Training
TRAIN_EU	Cost of training the trainers for end users	Training	Training
TRAIN_SL	Cost of training the trainers for system level staff	Training	Training
UC_CLASS	Daily cost of class (Max.: 10 students)	Internal	Training
UC_STUDENT	Daily cost of training one trainer	Internal	Training
INST	Total cost of NIBRS installation	Install	Install
INST_HW	Cost of hardware installation	Install	Install
INST_SW	Cost of software installation	Install	Install
INST_CIR	Cost of circuit installation	Install	Install
UC_PORT	Unit cost for installation of cabling and wall ports	Internal	Install
Q_WKS	Number of additional RMS workstations needed for the NIBRS	RMS	Assumptions Install
Q_PTR	Number of additional printers required for RMS/NIBRS participation	RMS	Assumptions Install
Q_RSC	Number of remote sites with insufficient connectivity	RMS	Assumptions Install
UC_SW_INST	Per day cost for installing COTS software	Internal	Install
Q_RS	Number of Remote Sites that will participate in the RMS/NIBRS	RMS	Assumptions Install Data Conv
CIR_SITE	Cost of circuit installation at remote site	Install	Install
CIR_HQ	Cost of circuit installation at headquarters site	Install	Install

Cost Model (Cont'd) Variable Name	Definition	Original Input Location	Worksheets Where Used
Q-RSC	Number of additional remote sites with no existing connectivity, or sites which require additional bandwidth for RMS/NIBRS	RMS	Install Telecom
DATACON	Total cost of data conversion	Data Conv	Data Conv
UC_DCS	One-time cost of data conversion for a small agency (stand-alone PC)	Internal	Data Conv
UC_DCM	One-time cost of data conversion for a medium agency (LAN but no WAN)	Internal	Data Conv
UC_DCL	One-time cost of data conversion for a large agency (LAN and WAN)	Internal	Data Conv
LEVEL	Support service on a 8 x 5 basis (level=1) or a 24 x 7 basis (level=2)	RMS Assumptions	SW Maint HW Maint
LAN	Corresponds to Multi-user (Yes or No)	RMS Internal	Hardware
CER_SW8	The CER used to estimate the cost of 8 x 5 maintenance support for software	Internal	SW Maint
CER_SW24	The CER used to estimate the cost of 24 x 7 maintenance support for software	Internal	SW Maint
SOLUTION	1=COTS 2=Custom	RMS Assumptions	SW Maint
HW	Total purchase price of equipment (system hardware)	Hardware	HW Maint
CER_HW8	The CER used to estimate the cost of 8 x 5 maintenance support for HW	Internal	HW Maint
CER_HW24	The CER used to estimate the cost of 24 x 7 maintenance support for HW	Internal	HW Maint
COM	Annual cost of telecommunications	Telecom	Telecom
COM_SITE	The annual cost of telecommunications of the remote sites	Telecom	Telecom

Cost Model (Cont'd) Variable Name	Definition	Original Input Location	Worksheets Where Used
COM_HQ	The annual cost of telecommunications of headquarters	Telecom	Telecom
RMS SERVER	Annual cost of RMS Server	Tables Hardware	Tables Hardware
YEAR	Current four-digit year; used to escalate labor cost from year 1999, when original cost model was completed	RMS	Internal

Table C.2 Look Up Table

Table Name	Purpose	Original Input Location	Worksheets Where Used	Bounds on Data
TB_STATE	Determines the number of staff months for custom SW development, based on the state of the current system	NIBRS SW	NIBRS SW	No bounds. State refers to current status of reporting system. Possible states are RMS, non-IBR RMS, or RMS IBR.
TB_SERVER	Determines server cost, based on concurrent users	Hardware	Hardware	The number of concurrent users ranges from 1-500 (inclusive). This table is used if the current system is a multi-user system, incidents per month and/or number of sworn officers are large, or if the concurrent user escalation factor is high.
TB_CIRCUIT	Determines the circuit charge for telecommunications	Telecom	Install Telecom	The breakpoint ranges from 0-769, while circuit size ranges from 64-1024

Appendix D: Commonly Used Acronymns

BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
CAD	computer-aided dispatch
CITA	Crime Identification Technology Act
CJIS	Criminal Justice Information Services Division of the FBI
COPS	Community Oriented Policing Services
COTS	commercial off-the-shelf (refers to software products)
DMV	Department of Motor Vehicles
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
GIS	geographical information system
GSA	General Services Administration
GUI	graphical user interface
GWAC	government-wide agency contract
HVAC	heating, ventilation, and air conditioning
IBR	incident-based reporting
ICD	interface control document
IT	information technology
LAN	local area network
MDC	mobile data computer (laptop)
MORE	Making Officer Redeployment Effective (a COPS program)
MTBF	mean time between failure
NCJRS	National Criminal Justice Reference Service
NIBRS	National Incident-Based Reporting System
NIJ	National Institute of Justice
O&M	operation and maintenance
OJP	Office of Justice Programs
POP	Point of Presence
RFI	request for information
RFP	request for proposal
RMS	records management system
SOW	statement of work
UCR	Uniform Crime Reporting
UNI	user network interface
UPS	uninterruptible power source
VAWFV	Violence Against Women and Family Violence
WAN	wide area network