Document Title:	Comprehensive Regional Information System Project Volume 3: A Practitioner's Handbook for Law Enforcement Information-Sharing Systems: Preliminary Requirements
Author(s):	Noblis
Document No.:	219379
Date Received:	August 2007
Award Number:	2001-LT-BX-K002

Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Providing Unbiased and Objective Technical Assistance

Enabling Criminal Justice Information Exchange

Modernizing Criminal Justice Processes

Center for
Criminal
Justice
Technology

Comprehensive Regional Information System Project
Volume 3

A Practitioner's Handbook for Law Enforcement Information-Sharing Systems: Preliminary Requirements

NOBLIS TECHNICAL REPORT
MTR-2006-037
Contract Number 2001-LT-BX-K002

noblis
For the best of reasons

Center for Criminal Justice Technology

MTR-2006-037
Noblis Technical Report

Comprehensive Regional Information-Sharing Project, Volume 3

A Practitioner's Handbook for Regional Law Enforcement Information-Sharing Systems: Preliminary Requirements

January 2007

NIJ
NATIONAL INSTITUTE of JUSTICE

Supported under Cooperative Agreement 2001-LT-BX-K002
Office of Science and Technology
National Institute of Justice
Office of Justice Programs
U.S. Department of Justice

Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Justice.

Noblis strives to provide the latest and most complete information in its documents and makes such documents available for informational purposes only. You may not copy or otherwise use this document or its contents for commercial gain. Noblis is not responsible for the uses you make of the information provided herein.

Websites and sources listed provide useful information at the time of this writing, but the authors do not endorse any information of the sponsor organization or other information on the websites.

Cover design by Mary Brick, Noblis

Photos courtesy of (from l to r): JupiterImages Corporation (1-2)
Harry Cummins, Noblis (3)

noblis™
For the best of reasons

3150 Fairview Park Drive South, Falls Church, VA 22042

This page intentionally left blank

EXECUTIVE SUMMARY

Many law enforcement agencies are interested in expanding the sharing of information with other law enforcement agencies throughout their region. A growing option to address this interest is an organized regional law enforcement information-sharing program; through this program, agencies access a regional law enforcement information-sharing system (ISS). There are a fair number of regional law enforcement ISSs already in use today with varying capability, functionality, and complexity. Studying these existing programs and systems provides an opportunity for other agencies that are considering a regional ISS to learn and understand what is needed to put such systems into place.

This Practitioner's Handbook was developed in conjunction with the Comprehensive Regional Information-Sharing Project (CRISP) being conducted by Noblis' Center for Criminal Justice Technology (CCJT), in partnership with the National Institute of Justice (NIJ). The purpose of the overall CRISP program is to examine "best practices in how information is currently being delivered within regional law enforcement ISSs." Based on research conducted as part of CRISP, no single source could be identified that provided extensive technical and non-technical requirements, policy requirements, and guidance for developing a regional law enforcement ISS that was independent of an ISS program already in place. This Practitioner's Handbook, which is one component of the CRISP effort, seeks to fill that void with a clear, documented set of requirements and guidelines. This handbook is based on input from law enforcement agencies that have experience with regional law enforcement information-sharing programs, as well as agencies that have never participated in such programs. Analyzing the current sharing practices and restrictions at agencies that have experience with regional law enforcement information-sharing programs provides the specific details for these requirements and guidelines. Input from non-participant agencies helps confirm best practices and lessons learned. It also allows requirements to be presented in a way that will ease transition to a regional law enforcement information-sharing program by prioritizing the ISS features that are most effective. These fundamental features and capabilities help determine the requirements that an ISS should meet.

Two primary research efforts were employed throughout the CRISP program: making site visits to six selected ISS programs and conducting a national survey of law enforcement agencies on information-sharing, resulting in approximately 200 responses. Requirements and guidance for an ISS and corresponding ISS program were developed from this extensive information-gathering effort. In 2005, six on-site interviews were conducted with key representatives from the following ISS programs (shown in the order the visits were conducted):

- Comprehensive Regional Information Management Exchange System (CRIMES), located in the Hampton Roads area of Virginia
- Factual Analysis Criminal Threat Solution (FACTS) system, based in Tallahassee, Florida
- Citizen and Law Enforcement Analysis and Reporting (CLEAR) system, based in Chicago, Illinois
- Florida Intelligence Site (InSite), based in Tallahassee, Florida
- Florida Information Network for Data Exchange and Retrieval (FINDER) system, based in Orlando, Florida
- Automated Regional Justice Information System (ARJIS), based in San Diego, California

Additionally, in partnership with the Police Executive Research Forum (PERF), a national survey was distributed to law enforcement agencies across the United States during the spring and summer of 2006. Agencies surveyed reflected a mix of ISS participants and non-participants and represented a range of geographic areas and agency sizes. Agencies responded to questions regarding general agency characteristics, methods that agencies currently use to share information, factors surrounding an agency's decision to participate in a regional ISS, information-sharing needs, desired capabilities of an ISS program, and lessons learned from agencies currently participating in an ISS program.

This handbook is primarily intended for law enforcement agencies that are considering undertaking a regional law enforcement ISS program and wish to better understand the capabilities that such systems should provide and the spe-

cific requirements that should be met. Those agencies currently participating in an ISS program may also benefit from consulting this handbook to identify possible enhancements to their ISS capabilities or operations. Further, technical consultants may use this handbook to assess ISS feasibility for a set of agencies and to develop a preliminary system design.

Acknowledgments

Many individuals contributed to the material in this document, and other CRISP companion documents. The authors first wish to thank the officers, detectives, crime analysts, and command staff who participated in site visits. Representatives from the organizations listed below provided detailed information that was collected as part of the overall CRISP effort and provided the basis for the information in this document:

- Automated Regional Justice Information System (ARJIS), based in San Diego, California
- Citizen and Law Enforcement Analysis and Reporting (CLEAR) system, based in Chicago, Illinois
- Comprehensive Regional Information Management Exchange System (CRIMES), located in the Hampton Roads area of Virginia
- Factual Analysis Criminal Threat Solution (FACTS) system, based in Tallahassee, Florida
- Florida Intelligence Site (InSite), based in Tallahassee, Florida
- Florida Information Network for Data Exchange and Retrieval (FINDER) system, based in Orlando, Florida

The authors would like to extend a special expression of thanks to the following individuals from the organizations above for the support they provided during site visits and for their review of other CRISP products:

- Ms. Pam Scanlon, Executive Director, ARJIS
- Mr. James Hickey, Project Manager, CLEAR
- Chief Mark Marshall, Mr. Dennis Mook, and Lt. Joseph Ribiero, CRIMES
- Chief Mark Zadra and Inspector Larry Shaw, FACTS/InSite
- Dr. Michael Reynolds and Dr. Ronald Eglin, FINDER

The authors also thank the members of the Police Executive Research Forum (PERF) who conducted the national survey and the focus group members who assisted in vetting the survey:

- Nathan Ballard, PERF, Research Assistant
- Mary Martinez, PERF, Research Assistant
- Apollo Kowalyk, PERF Fellow, Edmonton Police Service, Alberta, Canada
- Kristin Kappelman, PERF, Research Associate
- Bruce Kubu, PERF, Senior Research Associate
- Bruce Taylor, PERF, Research Director
- Captain Jack Anderson, Sheriff's Department, Orange County, California
- Jim Austin, Special Agent, Naval Criminal Investigative Service, Washington, D.C.
- Lorelei Brown, Manager, Strategic Planning Section, Sheriff's Office, Hillsborough County, Florida
- Assistant Chief Cindy Combs, Police Department, Cincinnati, Ohio
- James Hickey, Project Manager, Criminal Justice Integration Project, Police Department, Chicago, Illinois
- Captain Jennifer Kilburn, Sheriff's Office, Jefferson County, Alabama
- Captain Alan Lee, Police Department, Prince George's County, Maryland
- Lieutenant Erich Miller, Metropolitan Police Department, Washington, D.C.
- Phil Ramer, Senior Research Associate, Institute for Intergovernmental Research, Tallahassee, Florida
- Bob Mosley, independent consultant, Metropolitan Washington Council of Governments

The authors also thank all of the law enforcement agencies who responded to the national survey. Their responses expanded our knowledge regarding the many information-sharing goals that law enforcement would like to meet.

The authors would like to acknowledge the contributions of the following individuals for their review of draft versions of this document and for the support they provided during the overall CRISP effort:

- Mr. Hyuk Byun, Program Executive, National Institute of Justice
- Ms. Michele Moses, Technical Program Analyst (contractor), National Institute of Justice

- Mr. William Ford, Program Manager, National Institute of Justice
- Mr. Phil Ramer, Senior Research Associate, Institute for Intergovernmental Research
- The members of the Global[1] Intelligence Working Group

[1] The Global Justice Information-Sharing Initiative (Global) serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information-sharing and integration initiatives. GLOBAL was created to support the broad-scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

List of Figures

List of Tables

This page intentionally left blank

1 Introduction

Recently identified weaknesses in information-sharing practices in the law enforcement community have highlighted the need to share information among local, state, and federal criminal justice agencies. The ability to access regional law enforcement data supports local efforts to identify and combat cross-jurisdictional crime and advances investigative efforts to identify case leads by gaining access to additional information. These regional systems can also provide local law enforcement with the information needed to support state and federal counterterrorism efforts.

Recognizing these needs, many law enforcement and justice agencies have established information-sharing systems (ISSs). These systems share electronic information from multiple jurisdictions, enabling law enforcement personnel to quickly gather information on cases and generate additional leads. Use of regional ISSs can result in increased time efficiency, which in turn can lead to significant labor savings. Law enforcement officers can devote more of their time to preventing and combating criminal activity, which replaces time spent tracking down information.

While regional efforts exist and continue to come online, there is only a limited amount of analysis regarding how these ISSs were developed and currently operate. Additional local and state agencies are seeking approaches and solutions that fit their situations and needs. If agencies that have not yet developed an ISS can learn from the experience gained and the lessons learned, they can adopt a strategy that works for them. Access to information about ISS implementation can benefit many agencies around the country.

This Practitioner's Handbook provides a preliminary set of functional and operational requirements and guidance to help agencies implement a regional law enforcement ISS. These requirements are considered preliminary because this handbook is based on the experiences of six regional law enforcement ISSs and the input from the approximately 200 law enforcement agencies that responded to a national survey. These requirements do not necessarily include all of the requirements that would be provided in a request for proposal (RFP) effort.

The handbook is based on input from agencies that have experience with regional law enforcement information-sharing programs and from agencies that have never participated in such programs. Current sharing practices and restrictions at agencies help drive requirements and guidelines, and input from participant and non-participant agencies can confirm best practices and lessons learned. This handbook presents requirements in a way that will help agencies develop a regional law enforcement information-sharing program and prioritize the requirements and guidelines. Agencies can start with the requirements that meet their needs and build upon others to better support their particular regional or local environment, laws, and technical infrastructure.

1.1 Background

As criminal activity and the threat of terrorism continue to impact the safety of individuals in this country, it becomes increasingly important that law enforcement agencies in the United States—regardless of size—appreciate the importance of information collection and sharing. Following the direction of federal recommendations and guidelines (such as the National Criminal Intelligence-Sharing Plan [NCISP]), the National Institute of Justice (NIJ) partnered with Noblis' Center for Criminal Justice Technology (CCJT) to identify best practices and to define the policy and programmatic concepts and functional, operational, and technical characteristics associated with sharing law enforcement information regionally. During 2005, Noblis conducted interviews with the following major regional law enforcement ISSs (see Figure 1-1):

- Comprehensive Regional Information Management Exchange System (CRIMES) in Hampton Roads, Virginia (June 2005)
- Factual Analysis Criminal Threat Solution (FACTS) in Tallahassee, Florida (September and October 2005)
- InSite system in Tallahassee, Florida (September and October 2005)
- Citizen Law Enforcement and Analysis Reporting (CLEAR) in Chicago, Illinois (October 2005)

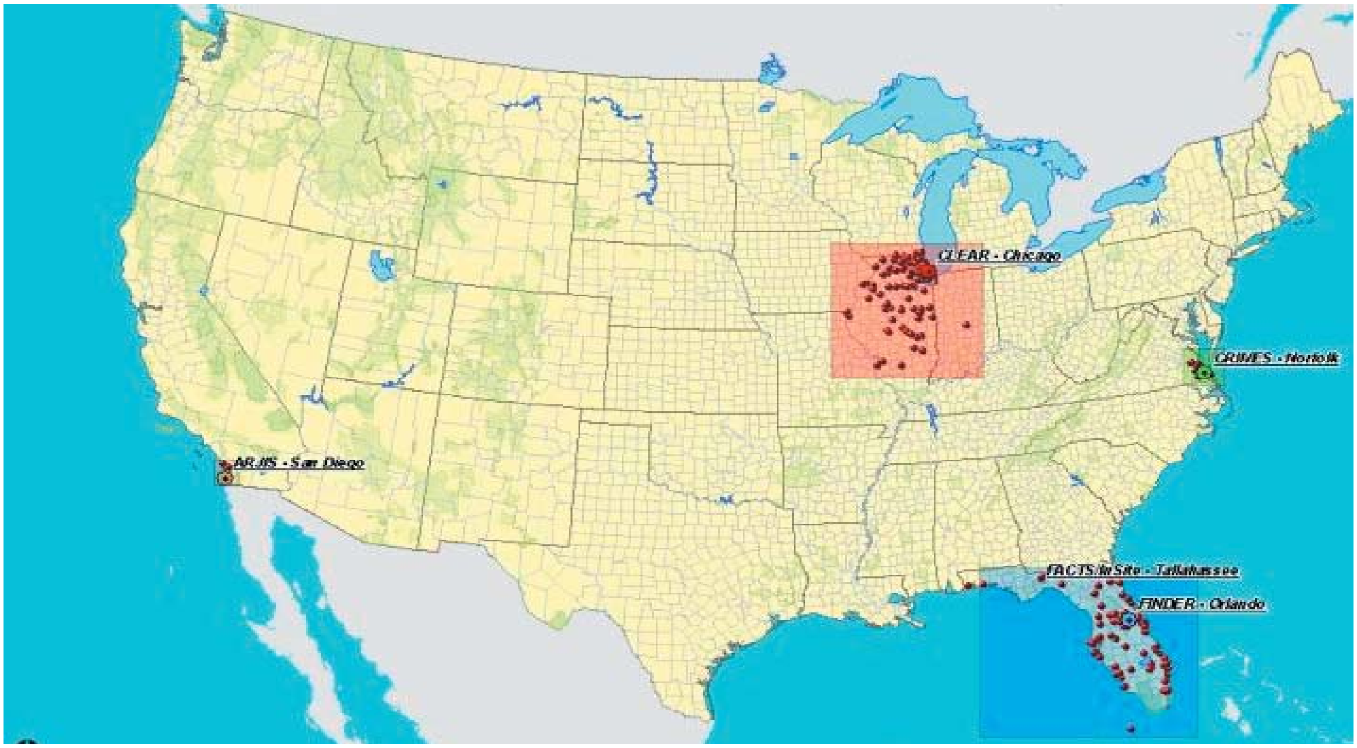

Figure 1-1. Overview Map of Surveyed Information-Sharing System Organizations

- Florida Integrated Network for Data Exchange and Retrieval (FINDER) in Orlando, Florida (November 2005)
- Automated Regional Justice Information System (ARJIS) in San Diego, California (November 2005)

These regional systems were selected based on certain shared characteristics that were identified including maturity and number of participating agencies. Interviews with these established ISSs provided a substantial set of best practices and lessons learned. The preliminary requirements described in this handbook are based, in part, on the success factors, recommendations, positive impacts, identified areas for improvement, and desired capabilities provided by the law enforcement and other personnel associated with the management and governance of these ISSs.

Additionally, the Comprehensive Regional Information-Sharing Project (CRISP) team worked with the Police Executive Research Forum (PERF) to distribute a national survey to law enforcement agencies around the country. Agencies surveyed reflected a mix of ISS participants and non-participants and represented a range of geographic areas and agency sizes. Agencies responded to questions regarding methods they currently use to share information, factors surrounding an agency's decision to participate in a regional ISS, desired capabilities of an ISS program and system, and lessons learned from agencies currently participating in an ISS program. More than 200 agencies completed the survey.

Figure 1-2—based on PERF national survey data—is an example of some of the information collected. The figure illustrates the type and priority associated with the sharing of various data categories. Although the ranking varies somewhat by ISS experience levels, the figure illustrates the desire by agencies to share all types of information.

This handbook is one component of the CRISP effort to provide potential system developers with initial guidance to define functional and operational requirements for developing regional ISSs for law enforcement. A list of other CRISP report documents is provided below; additional information about these reports can be found in Appendix C of this document:

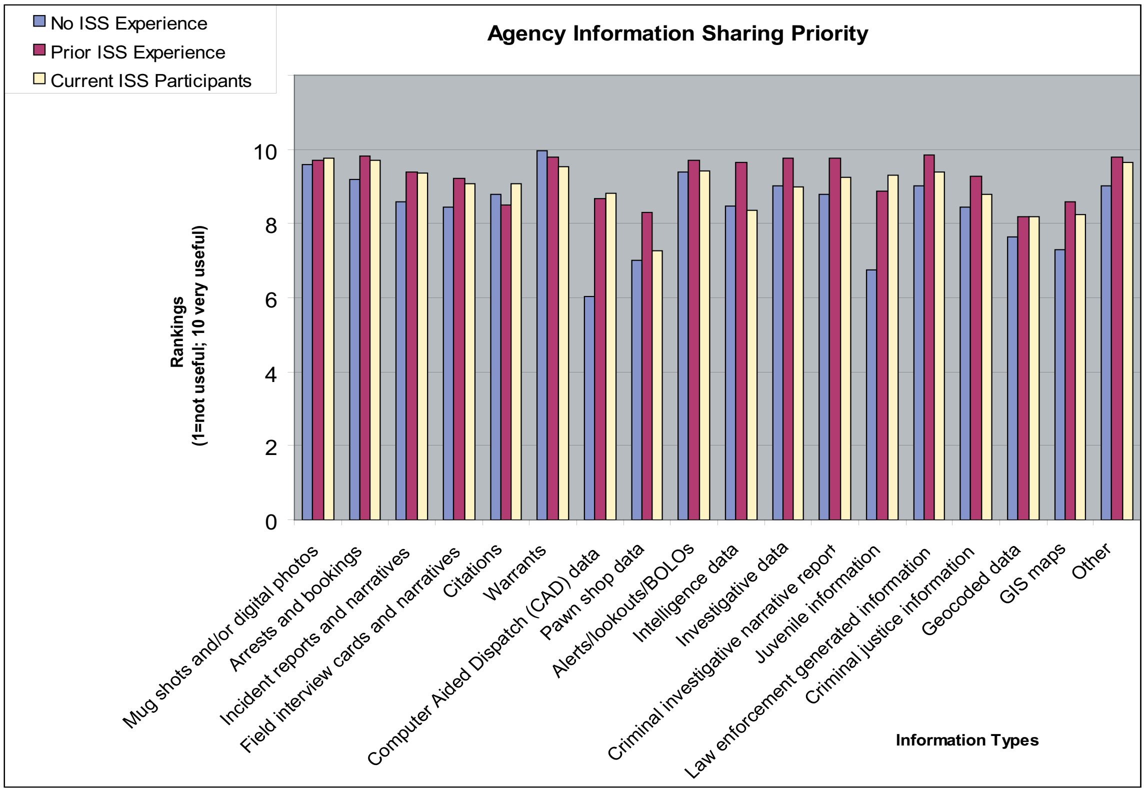

Figure 1-2. Agency Information-Sharing Priority

- *Concept of Operations (CONOPS)*: Describes best practices in establishing and operating regional law enforcement ISSs.
- *CRISP Mapping Application*: Provides a visual means to view and compare information on the six interviewed ISSs.
- *Metrics for Law Enforcement Information-Sharing Systems*: Examines the use of metrics as a tool to assess the effectiveness of a law enforcement ISS and its impact on operations.

1.2 Objectives

This handbook is structured to fulfill two key objectives:

- Provide understanding
  - Identify best practices that can guide the development of an effective ISS
  - Describe main ISS technical and non-technical features
  - Identify feasible functions and operations of an ISS
- Provide guidance
  - Enhance or expand an existing ISS
  - Define ISS requirements
  - Facilitate the request for information (RFI), request for proposal (RFP), and other components of the planning, design, acquisition, and implementation processes

  - Develop a single source of ISS information that contains extensive technical and non-technical requirements, policy requirements, and guidance that is independent of a particular regional ISS program in place

The primary audience for this handbook is the law enforcement agency or set of agencies that is considering implementing a regional law enforcement ISS and wants to better understand what is needed to put such a program and system into place. Individuals or agencies currently participating in an operational ISS, as well as those not participating in an ISS, can also benefit from this handbook. Those currently participating in an ISS program can use the handbook to identify possible enhancements to their ISS capabilities or operations. Those not currently participating in an ISS program can use this handbook, along with other CRISP products, to assess the feasibility of developing an ISS.

1.3 Assumptions and Constraints

This handbook is primarily based on the interviews conducted and information gathered during onsite visits to the six selected regional ISSs, as well as the national survey responses received from approximately 200 law enforcement agencies. While the language of this handbook resembles a set of specifications, it is intended to be used by law enforcement practitioners as a set of guidelines for implementing or joining an ISS program. The preliminary requirements presented here are recommended as guiding principles that may be adapted by practitioners or realigned based on the environment of the potential ISS. This handbook presents the best practices of establishing or joining a regional law enforcement ISS based on extensive research of a variety of law enforcement agencies and their information-sharing practices and needs.

A few of the terms used throughout the document are defined below so that their intended meaning is interpreted consistently. A complete glossary is provided in Appendix A.

- **Information Exchange/Exchange Information.** Giving *and* receiving of information
- **Information-Sharing/Share Information.** Giving *and/or* receiving of information
- **Information-Sharing System.** A collection of software and hardware components used to perform information-sharing functions as well as the support (system administration) needed to operate the components
- **Information-Sharing System Program.** The effort encompassing the ISS, users, policies for managing and using the system, and operations to which the system is applied
- **Region.** Area consisting of law enforcement agencies with which one may coordinate activities; may extend over city, county, or state boundaries; a multi-jurisdictional area
- **Regional Law Enforcement Information-Sharing System.** Electronic system containing information originating from local or state law enforcement agency records management systems that is shared among law enforcement agencies within a region

1.4 Document Organization

This handbook includes seven sections and three appendices. To help the reader understand how the requirements relate to the law enforcement operational environment, real-world law enforcement scenarios are presented that relate to law enforcement work processes. The scenarios contain explicit law enforcement requirements that are broken down into functional and operational ISS requirements in subsequent sections. ISS program organization, considerations for implementing a regional law enforcement ISS, and the methods for evaluating an ISS program's value are presented in the sections that follow the requirements.

Section 2 provides a high-level overview of an ISS and explains the approach taken to develop preliminary requirements and guidance. Section 3 presents real-world law enforcement operational scenarios; each scenario is followed by a list of derived requirements, categorized as functional or operational. These requirements illustrate how explicit

ISS requirements can be identified. Section 4, Functional ISS Requirements, describes the fundamental capabilities that must be met to realize an effective ISS. Section 5, Operational ISS Requirements, describes the technical specifications needed to implement an effective ISS. Section 6 focuses on considerations—such as governance, management, membership, and funding—for implementing an ISS; these considerations address programmatic aspects of an ISS program that may not be explicitly presented in the scenarios of Section 3 but are strongly recommended for review prior to establishing or joining an ISS program. Section 7 summarizes best practices for capturing the metrics of an ISS and for evaluating the value added by implementing an ISS, as presented in the *Metrics for the Evaluation of Law Enforcement Information-Sharing Systems* document.

Appendix A provides a glossary of terms and a list of acronyms used throughout this handbook. Appendix B illustrates how certain ISS capabilities and requirements map to the NCISP recommendations that were considered when developing this handbook. References are listed in Appendix C.

This page intentionally left blank

2 ISS Overview and Approach

A regional law enforcement ISS combines the necessary software and hardware components to perform information-sharing functions and provides the support (system administration) needed to operate the components. A regional law enforcement ISS program encompasses the ISS and the components needed to oversee the implementation, maintenance, and expansion of the ISS such as governance, management, policies/procedures and financial support. This section provides a high-level description of an ISS and the architectural options that must be considered. It also describes the approach taken to develop ISS functional and operational requirements and guidance.

2.1 General Description of an ISS

This section provides a high-level overview of the components and functions of a typical ISS as they pertain to law enforcement.

2.1.1 ISS Components

The ISS consists of hardware and software elements that support the functionality of the ISS. The hardware components include a data repository, a data management processor, an application processor, user workstations, and a communications network. The software components include the operating system, application software, database management software, and communication/network software.

2.1.2 ISS Architectures

A key component of any ISS is the technical architecture that provides the infrastructure for exchanging and accessing data. These hardware and software components are normally organized into one of three ISS architectural models: centralized, distributed, or hybrid. Although there are basic functional and operational requirements for any ISS, each model has unique considerations that should be addressed. Each approach has advantages and disadvantages that may or may not map well into a region's technical, political, legal, or financial environment. The following sections provide a high-level overview of the architectural approaches. A more detailed discussion of the alternative ISS architectures can be found in the *CRISP Concept of Operations (CONOPS)*, a companion document.

2.1.2.1 Centralized Architecture

In the centralized architecture model, data from contributing ISS law enforcement agencies is stored in a centralized repository, which allows the ISS to have a main point of access and a central location where data can be managed. With the centralized approach a data warehouse typically stores records contributed by member agencies. Each agency can access the central database to enter information and to research case data.

Figure 2-1 illustrates a centralized architecture model.

In the distributed architecture model, the data from contributing ISS law enforcement agencies is stored in local data repositories at the participating agencies. The distributed approach implements a query mechanism that allows participating ISS members to view information gathered throughout the region while allowing each agency to retain control over their local data. Each participating agency acts as an endpoint to the ISS and responds to a search request issued by the ISS.

Figure 2-2 illustrates a distributed architecture model.

A hybrid architecture model combines features of the centralized and distributed models. A hybrid approach makes it possible to have some centralized data sources while also providing access to distributed information sources. Centralized data sources would consist of the types of data that most users want to query and analyze frequently. In this model, data from the central repository is extracted and stored in a separate data repository or data warehouse, where data storage (updates) and retrieval (query) operations are performed.

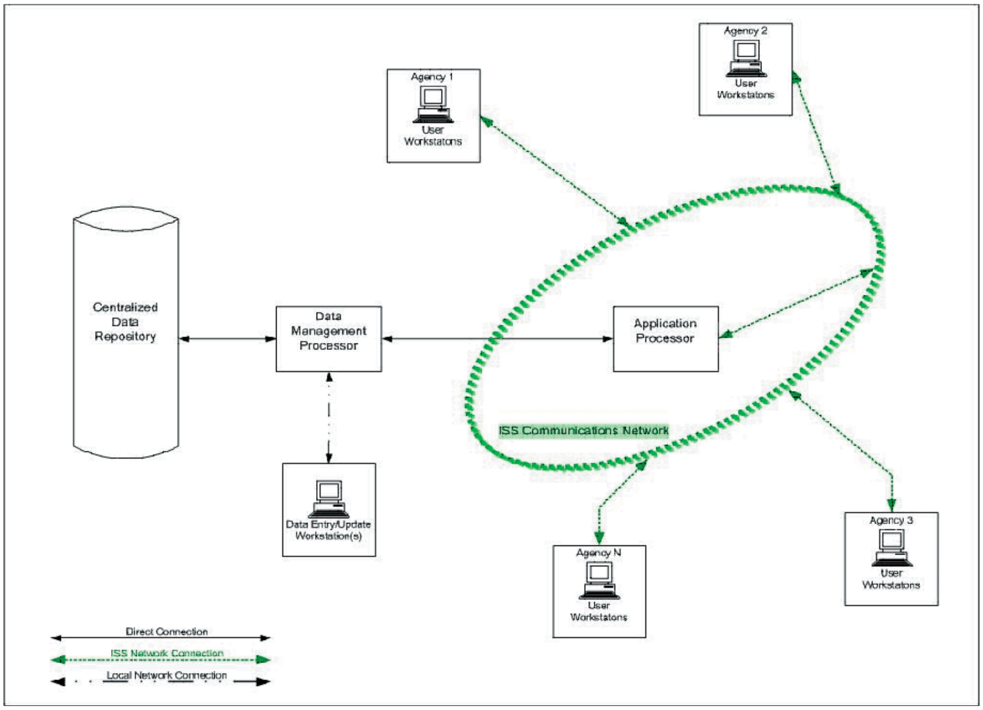

Figure 2-1. Example of a Centralized Architecture Model

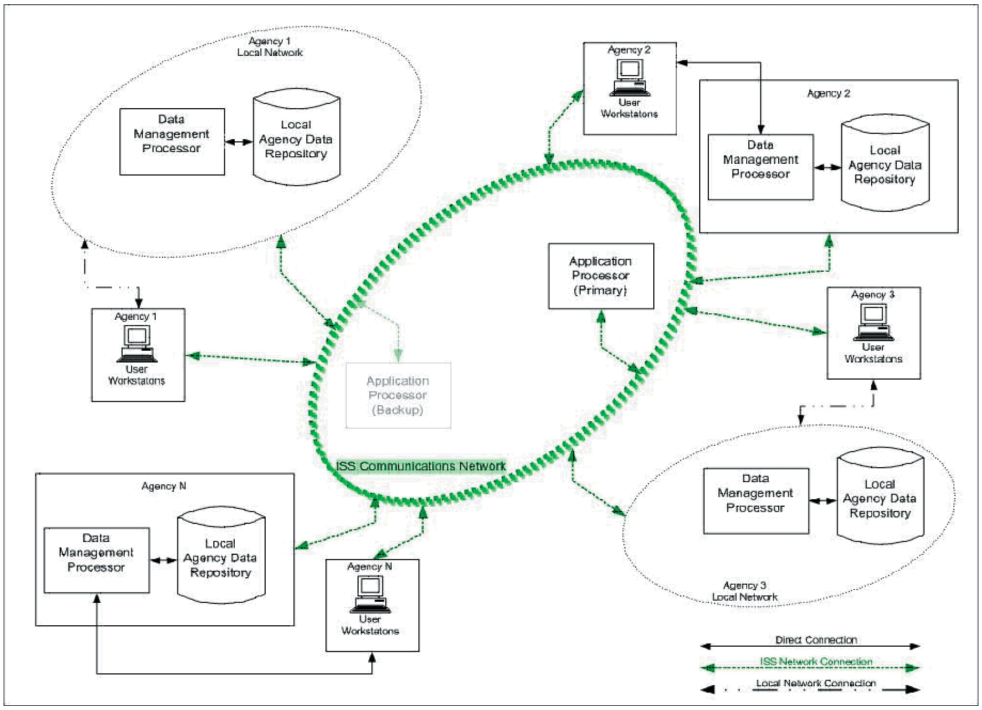
Agency 1
Local Network
Data Management Processor
Local Agency Data Repository
Agency 2
User Workstatons
Agency 2
Data Management Processor
Local Agency Data Repository
Application Processor (Primary)
Agency 1
User Workstatons
Application Processor (Backup)
Agency 3
User Workstatons
ISS Communications Network
Agency N
Data Management Processor
Local Agency Data Repository
Data Management Processor
Local Agency Data Repository
Agency 3
Local Network
Agency N
User Workstatons
Direct Connection
ISS Network Connection
Local Network Connection

Figure 2-2. Example of a Distributed Architecture Model

Figure 2-3 illustrates the hybrid architecture model.

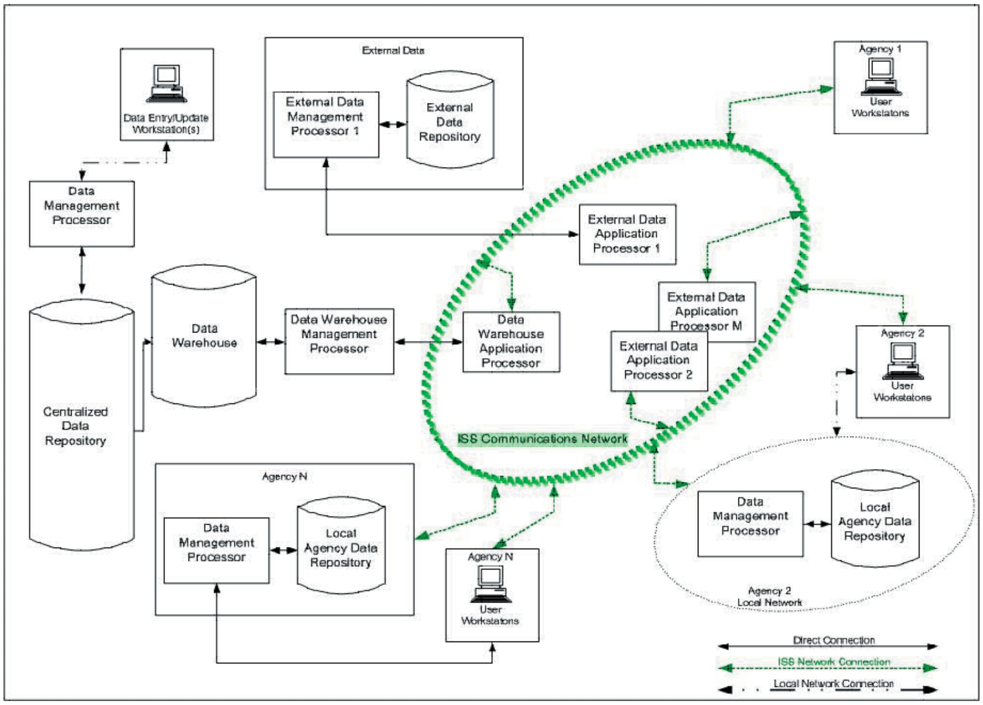
Data Entry/Update Workstation(s)
External Data
External Data Management Processor 1
External Data Repository
Agency 1
User Workstations
Data Management Processor
External Data Application Processor 1
Centralized Data Repository
Data Warehouse
Data Warehouse Management Processor
Data Warehouse Application Processor
External Data Application Processor M
External Data Application Processor 2
Agency 2
User Workstations
ISS Communications Network
Agency N
Data Management Processor
Local Agency Data Repository
Agency N
User Workstations
Data Management Processor
Local Agency Data Repository
Agency 2 Local Network
Direct Connection
ISS Network Connection
Local Network Connection

Figure 2-3. Example of a Hybrid Architecture Model

2.1.3 ISS Functions

The main function of a regional law enforcement ISS is to provide a mechanism for law enforcement agencies at the local, state, and federal levels to exchange information. There are a number of objectives for information-sharing, as illustrated in Figure 2-4.

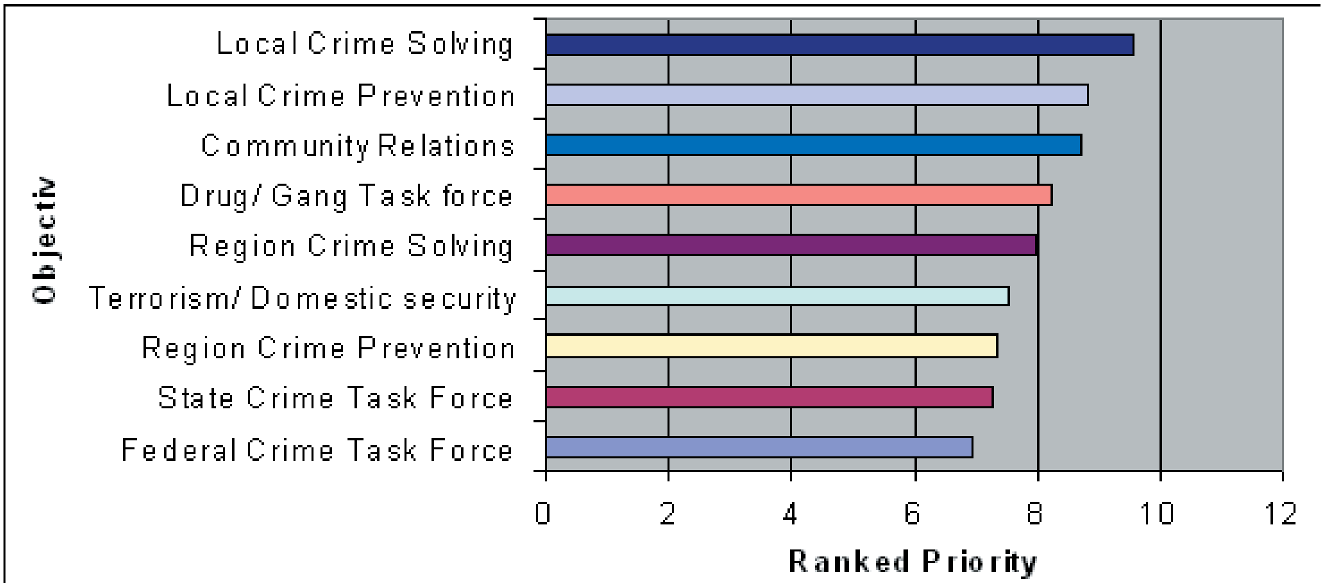

Figure 2-4. Objectives of Information-Sharing

In order for the ISS to be effective in meeting these objectives, however, it must be populated with a critical mass of law enforcement data. To accomplish this, the ISS should use a data aggregation method that accepts law enforcement data from all participating agencies. Users should be able to query the system for a variety of data that could potentially help investigators identify case leads, proactively deploy resources, and increase patrol officer safety. Users should also be able to request reports detailing query-returned data. Another key function is the ability of the ISS to de-conflict stored data so users are not presented with contradictory information. A more in-depth discussion of the functions of regional law enforcement ISSs is provided in Section 4.

2.2 Approach to Developing Requirements and Guidance

The approach taken to develop this set of preliminary requirements and guidance for regional law enforcement ISSs grew out of work done previously to develop specifications for internal law enforcement information systems and for communications interoperability.

2.2.1 Developing Requirements

Various techniques were considered for compiling the extensive information gathered and for developing requirements. One technique employed to develop the requirements for an ISS is the use of business cases or use cases; this approach was used to develop the Law Enforcement Information Technology Standards Council (LEITSC) Records Management System (RMS) and Computer-Aided Dispatch (CAD) specifications.[2] Another technique of particular interest is the use of scenarios, an approach used for the SAFECOM Statement of Requirements for Public Safety Wireless Communications and Interoperability specification.[3] Both of these techniques rely upon the relationships between work processes and requirements.

This handbook draws upon the techniques from both the LEITSC and SAFECOM documents and utilizes a tiered approach to requirements development. As shown in Figure 2-5, this tiered approach involved five activities:

- Gather information on work processes
- Develop real-world, user-specific scenarios
- Extract derived requirements from scenarios
- Identify explicit ISS functional and operational requirements
- Trace ISS requirements to specific ISS system capabilities

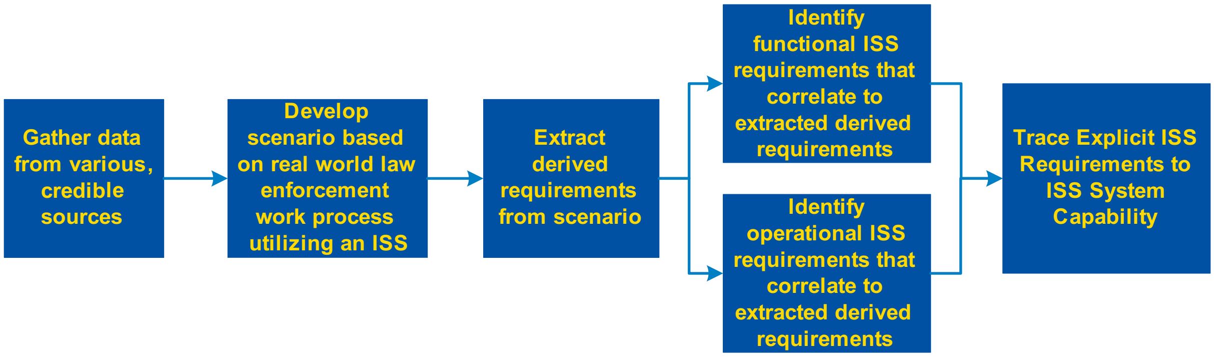
Gather data from various, credible sources
Develop scenario based on real world law enforcement work process utilizing an ISS
Extract derived requirements from scenario
Identify functional ISS requirements that correlate to extracted derived requirements
Identify operational ISS requirements that correlate to extracted derived requirements
Trace Explicit ISS Requirements to ISS System Capability

Figure 2-5. CRISP Tiered Approach to Regional Law Enforcement ISS Requirements Development

[2] Appendix C, References 12, 13

[3] Appendix C, Reference 11

The scenarios developed were based on acceptable policies and procedures for reporting, accessing, and using law enforcement information. Therefore, the set of requirements outlined in this handbook were developed with real-world law enforcement operational scenarios in mind. The content of the scenarios were derived from information gathered through the onsite ISS visits and the national survey. These scenarios, which were reviewed by former law enforcement officers, attempt to span the spectrum of law enforcement roles in an effort to highlight the added value an ISS can bring to law enforcement operations.

From the illustrated scenarios, requirements are derived and categorized as functional or operational. Functional requirements describe what the user should be able to do with the ISS in the work process. Operational requirements describe what the ISS should do to enable the user to perform the work process. For example, the ability for an officer to query an ISS from a mobile data terminal (MDT) is an example of a derived functional requirement in a given scenario. These derived requirements are then used as the foundation for identifying explicit functional and operational ISS requirements. The explicit functional and operational ISS requirements consist of the specifications necessary to realize the derived requirements referenced in the scenarios. For example, in order for the officer to query the ISS from the MDT, the ISS must have a user interface (an explicit functional requirement), and the user must have connectivity to the ISS via an MDT (an explicit operational requirement).

During the design phase of an ISS implementation, the explicit functional and operational requirements would be traced to the specific system feature that provides the required capability; this is done to ensure the system meets all ISS requirements. In Section 3, as each scenario is presented, work processes are traced at a very high-level to the appropriate functional or operational requirement. Figure 2-6 provides an example of the process of extracting a derived requirement from a given scenario and tracing it to its explicit ISS functional and operational requirements. The sample scenario referenced in Figure 2-6 is presented in its entirety in Section 3.1.

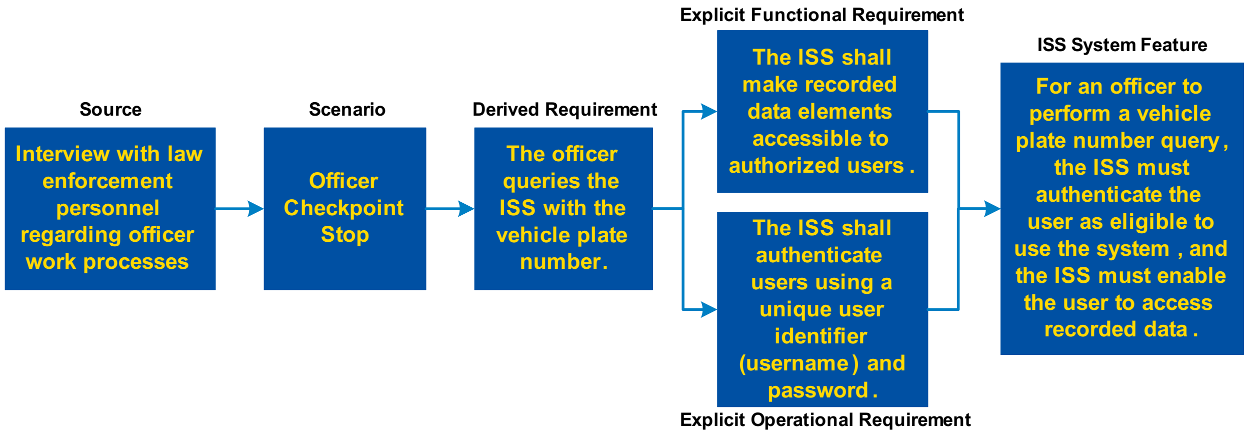
Source
Interview with law enforcement personnel regarding officer work processes
Scenario
Officer Checkpoint Stop
Derived Requirement
The officer queries the ISS with the vehicle plate number.
Explicit Functional Requirement
The ISS shall make recorded data elements accessible to authorized users .
The ISS shall authenticate users using a unique user identifier (username) and password.
Explicit Operational Requirement
ISS System Feature
For an officer to perform a vehicle plate number query, the ISS must authenticate the user as eligible to use the system , and the ISS must enable the user to access recorded data .

Figure 2-6. Example of CRISP Tiered Approach to Regional Law Enforcement ISS Requirements Development

2.2.2 Developing ISS Program Guidance

Guidance developed for this handbook pertains primarily to the operation of an ISS program. The goal for establishing guidance is for all agencies participating in an ISS program to experience benefits from using the ISS in day-to-day operations and to do so in a fair and equitable manner. Therefore, this handbook provides guidance in two key areas: ISS program organization and ISS program evaluation.

Best practices identified from the CRISP information-gathering effort, as well as the scenarios used to develop requirements, were the foundation for the guidance provided. A definitive set of requirements for guidance were not established as part of this effort. In some cases, the explicit ISS functional and operational requirements drive the guidance. In other cases, guidance is driven by policy and procedure currently in place at individual agencies, especially where legal and privacy policies are already in place. Given that an agency has its own set of policies and procedures, the extent to which specific guidance may be applied at an agency level will vary by agency. Another consideration when developing guidance is the inclusion of stakeholders—such as the ISS governance body, ISS management, agency management, end users, and ISS technical support—in the ISS program. ISS program advocates and funding entities may also be considered among the stakeholders. Therefore, guidance may be directed at the ISS program level, agency level, or both.

The guidance presented in Section 6 addresses the following topics related to ISS program implementation and operation:

- Programmatic Considerations, including
  - Governance
  - Management
  - Public access
  - Funding
- Technical Considerations, including
  - ISS architecture
  - Key system capabilities
  - Non-law enforcement data sources
  - Software ownership
  - Vendor and technology changes

Guidance on ISS program evaluation, presented in Section 7, addresses metrics evaluation methodology specific to a law enforcement ISS program. ISS program evaluation is an organizational element and may be applied to all aspects of the ISS program. Guidance in this area is presented in its own section due to its complexity and the extensive metrics work that the CRISP project has conducted.

3 Law Enforcement ISS Scenarios

As introduced in Section 2, requirements were developed using a tiered approach. This approach relies upon user-specific scenarios to help identify ISS requirements. These scenarios illustrate how the adoption of an ISS can benefit law enforcement practices. The 12 scenarios presented in this section highlight use of an ISS across a wide range of law enforcement operations. The scenarios presented are used to frame functional and operational capabilities of an ISS and incorporate fundamental requirements for functions and features that are necessary for an ISS to be effective, as well as optional requirements for features that add value to an ISS program.

Those planning the implementation of an ISS should consider the scenarios as examples of real-world events and work processes that derive a set of functional requirements, operational requirements, and policies and procedures for an ISS. Depending upon the applicability of the scenarios, those leading the implementation effort may choose a combination of options for deriving functional requirements, operational requirements, and policies and procedures for their ISS:

- *Adopt the scenarios* as a foundation for determining functional requirements, operational requirements, and policies and procedures for their ISS.
- *Adapt the scenarios* to better characterize the work environment and work processes, so they complement the involved personnel. The given scenarios may resemble but not fully reflect some law enforcement work processes. Scenarios may also be adapted to account for law enforcement or other user roles not addressed in this handbook. The adapted scenarios may then be used as a foundation for determining functional requirements, operational requirements, and policies and procedures for their ISS.
- *Develop additional scenarios* to better reflect the broad spectrum of law enforcement work processes. The scenarios presented may be used as a foundational set and a model for additional scenarios to be developed, as appropriate. Additional scenarios may be developed to account for other law enforcement or user roles not addressed in this handbook. The additional scenarios may then be used as a foundation for determining functional requirements, operational requirements, and policies and procedures for their ISS.

Many of the work processes in the 12 scenarios are operations that an ISS could support. Therefore, these work processes are used to illustrate how explicit requirements would be derived for the ISS to meet. Following each scenario is a requirements table consisting of three columns:

1. **Derived Requirement.** Derived requirement from work process illustrated in the scenario. These requirements are displayed in bold throughout each scenario and represent capabilities that could be implemented for an ISS.
2. **Requirement Type.** Classifies the requirement that would be associated with the work process as functional or operational or as a policy and procedure consideration. Functional and operational requirements are expanded in Section 4 and Section 5. Policies and procedure are steps in the work process that do not lead to functional or operational requirements but do specifically relate to ISS policies and procedures. Policy and procedure steps are addressed as guidance, not formal requirements, in Section 6.
3. **Law Enforcement Role.** Indicates the law enforcement entity performing the work process associated with the derived requirement. The term “system function” is used in cases where the ISS would perform the capability associated with the derived requirement.

3.1 Scenario 1: Patrol Officer Checkpoint Stop

A patrol officer stops a driver at a checkpoint and asks for a driver’s license, vehicle registration, and proof of insurance. Having **access to an MDT with ISS connectivity** and National Crime Information Center (NCIC) connectivity,[4] the patrol officer runs the vehicle registration tag number through the NCIC database. NCIC indicates that the vehicle is stolen. Through questioning, the officer determines that the driver is not authorized to drive the vehicle. The patrol officer proceeds to arrest the driver and impounds the vehicle.

While still at the checkpoint stop, the patrol officer **queries the regional ISS with the vehicle registration tag number** to determine any additional criminal activities involving the vehicle. The **ISS results show that the vehicle was seen leaving the scene of a reported narcotics case** in the jurisdiction of another agency participating in the ISS. According to the information returned by the ISS, the narcotics case involves an ongoing investigation of drug trafficking. The arrested driver also matches the **physical description, provided by the ISS, of the driver of the vehicle at the narcotics scene. ISS results also include the name and contact information of the investigator assigned to the case.** The patrol officer inventories the vehicle and finds drugs. The patrol officer contacts the investigator assigned to the narcotics case and validates the information. He enters his incident, with arrest, report into his agency's data repository. His **incident report—including the arrest report—is subsequently made available in the ISS.**

The investigator assigned to the narcotics case queries the ISS using the vehicle registration tag number. The **ISS returns the patrol officer's incident, with arrest, report through the ISS,** and **queries the ISS for additional information pertaining to the arrested driver.** The **ISS,** which now also contains the driver's true identity and a mug shot, **returns the arrested driver's known associates** and **displays a map showing any known addresses,** providing leads for the investigator to pursue.

Derived requirements from this scenario are shown in Table 3-1.

Table 3-1 Scenario 1 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Access to MDT with ISS connectivity	Operational	Patrol Officer
Queries regional ISS with vehicle registration tag number	Functional	Patrol Officer
ISS results show that the vehicle was seen leaving the scene of a reported narcotics case	Functional	System function
Physical description, provided by the ISS, of driver of vehicle at the narcotics scene	Functional	System function
ISS results include name and contact information of investigator assigned to associated case	Functional	System function
Incident report, including arrest report, are subsequently made available in ISS	Operational	System function
Searches ISS using vehicle registration tag number provided by patrol officer	Functional	Investigator
ISS returns patrol officer's incident, with arrest, report through ISS	Functional	System function
Queries ISS for additional information pertaining to arrested driver	Functional	Investigator
ISS returns arrested driver's known associates	Functional	System function
ISS displays a map showing any known addresses	Functional	System function

[4] Connectivity to external data repositories, such as NCIC, may be available to users without any correlation to the ISS. However, there is an option to offer users the capability to access such external data repositories (external to the ISS) through the ISS via an application. This refers to a "one-stop shopping" scheme that enables users to access multiple data repositories via one system interface.

3.2 Scenario 2: Investigator Burglary Case

A 911 Call Center receives a call reporting a burglary involving stolen property. Dispatch directs a patrol officer to the reported address. Upon arriving at the location, the patrol officer requests that an investigator come to the scene. An investigator arrives and begins interviewing the complainant and additional people at the burglary scene.

Back at her desk, the investigator **queries the regional ISS about the item that was stolen—a bicycle.** From the interviews at the burglary scene, the investigator learned that the bicycle was a woman's green, 20-speed manufactured by Schwinn. Since the **ISS has access to pawn data,** the **pawn records are displayed in response to the investigator's queries.** The ISS returns data stating that a bicycle matching the description from the burglary scene was pawned one day after the burglary, three counties away (within the ISS region).

The investigator **goes to the listed pawn shop to validate the pawn slip.** After validating the pawn slip and determining that the pawned bicycle is the same bicycle stolen from the burglary, she acquires an arrest warrant for the suspect. Since the investigator does not have access to the ISS from the field, she contacts her partner (or assigned personnel) at the precinct and asks him to **query the ISS using the name of the suspect.** The **ISS returns hits on the suspect, supplying the partner with the suspect's known associates and their last known addresses.** He relays this information to the investigator, who uses this data to locate and arrest the suspect.

Derived requirements from this scenario are shown in Table 3-2.

Table 3-2 Scenario 2 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Queries the regional ISS about the stolen property, a bicycle	Functional	Investigator
ISS has access to pawn data	Operational	System function
Pawn records are displayed in response to the investigator's queries	Functional	System function
Goes to the listed pawn shop to validate the pawn slip	Policy and Procedure	Investigator
Query the ISS using the name of the suspect	Functional	Investigator
ISS returns hits on the suspect supplying the partner with the suspect's known associates and their last known addresses	Functional	System function

3.3 Scenario 3: Crime Analyst Robbery Pattern

A patrol officer pulls over a white pickup truck for speeding. When asking for the driver's license and registration, the patrol officer notices a large bag of ball bearings on the front passenger seat. The officer issues the driver a traffic citation.

A few days later, a crime analyst reviews the physical evidence from a recent convenience store robbery. The related incident report shows that ball bearings were used to break the windows of the store. She **queries the ISS with keywords pertaining to the case** (e.g., "ball bearings", "robbery", "convenience store"). The **ISS returns multiple reports on convenience store robberies involving ball bearings.** Upon further review of the returned cases, the crime analyst notices that witnesses placed a white pickup truck outside several of the robbed stores.

The crime analyst prepares a report of her findings—with respect to the robbery pattern—for the agency's next CompStat meeting. After being informed of the pattern, Command Staff alerts all officers of the series of convenience store robberies involving ball bearings and potentially a white pickup truck. The **crime analyst makes her report—along with an alert—available to the ISS.**

The patrol officer who stopped the white pickup truck is on patrol when he **receives the crime analyst's alert via the ISS.** The patrol officer informs the crime analyst of the incident with the speeding, white pickup truck he stopped just a few days prior. The patrol officer also **prepares a narrative, which is made available to the ISS.** The crime analyst, in turn, relays this information to the detective assigned to the series of convenience store robberies. The detective **queries the ISS to retrieve the patrol officer's narrative and traffic citation. The ISS provides the detective with the driver's address, contact information, and any associates' information. After verifying the incident report with the patrol officer,** the detective uses the information provided by the ISS to locate the driver, now a suspect.

Derived requirements from this scenario are shown in Table 3-3.

Table 3-3 Scenario 3 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Queries the ISS with keywords pertaining to the case	Functional	Crime Analyst
ISS returns multiple reports on convenience store robberies involving ball bearings	Functional	System function
Crime analyst makes her report, along with an alert, available to ISS	Functional	Crime Analyst
Receives the crime analyst's alert via the ISS	Functional	System function
Prepares a narrative, which is made available to the ISS	Functional	Patrol Officer
Queries the ISS to retrieve the officer's narrative and traffic citation	Functional	Detective
ISS provides the detective with the driver's address, contact information, and any associates' information	Functional	System function
Verifies the incident report with the patrol officer	Policy and Procedure	Detective

3.4 Scenario 4: Crime Analyst Data/Statistics

A crime analyst **queries a regional ISS for various crime data and statistics** (drug incidents, stolen property, etc.). Since **there is a standardized set of crime types within the ISS,** the **ISS is able to return comprehensive crime incidents based on the analyst's search criteria.** The crime analyst **narrows her search by specifying locations.**

The **ISS returns recorded criminal activities at queried locations.** The crime analyst reviews the crime incidents

returned by the ISS, **maps the incidents** using the ISS mapping capability, identifies trends, and **maps the hot spots,** potentially projecting where subsequent criminal activities will likely occur. Command Staff uses this information to deploy officers to specified locations to monitor any suspicious activity or any potential suspects.

Derived requirements from this scenario are shown in Table 3-4.

Table 3-4 Scenario 4 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Queries a regional ISS for various crime data/statistics	Functional	Crime Analyst
There is a standardized set of crime types within the ISS	Functional	System function
ISS is able to return comprehensive crime incidents based on the analyst's search criteria	Functional	System function
Narrows her search by specifying locations	Functional	Crime Analyst
ISS returns recorded criminal activities at queried location	Functional	System function
Maps the incidents	Functional	Crime Analyst
Maps the hot spots	Functional	Crime Analyst

3.5 Scenario 5: Patrol Officer Field Interview

A patrol officer notices an individual outside a closed appliance store. The patrol officer approaches the individual and asks for identification and reason for being there. The patrol officer asks the individual to wait while he checks the individual's identification. While the individual waits, the patrol officer has **access to a personal data assistant [PDA] with ISS connectivity and queries the regional ISS with information from the identification provided by the individual.** The **ISS returns the individual's criminal history,** but there are currently no active warrants for the individual.

The patrol officer recalls from roll-call that there have been a series of appliance store burglaries in the general vicinity. The patrol officer **queries the ISS providing the general location and using the keywords "appliance store."** The patrol officer **retrieves the physical description and surveillance photos from one of the reports returned by the ISS,** and all resemble the individual now outside the appliance store. The patrol officer has reasonable suspicion to detain the individual more deliberately. He decides to call the detective assigned to the case, **whose name the patrol officer retrieves from the ISS.** The patrol officer describes the incident and the individual to the detective, who requests that the officer transport the individual to headquarters for questioning.

Derived requirements from this scenario are shown in Table 3-5.

Table 3-5 Scenario 5 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Access to a PDA with ISS connectivity	Functional	System function
Queries the regional ISS with information from the identification provided by the individual	Functional	Patrol Officer
ISS returns the individual's criminal history	Functional	System function
Queries the ISS with the general location and using the keywords "appliance store"	Functional	Patrol Officer
Retrieves the physical description and surveillance photos from one of the reports returned by the ISS	Functional	Patrol Officer
Retrieves detective's name from the ISS	Functional	Patrol Officer

3.6 Scenario 6: Patrol Officer Moving Violation Stop

A patrol officer pulls over a vehicle with a broken tail light. Before approaching the vehicle, the patrol officer runs the vehicle registration tag number in NCIC (on her MDT), which states the vehicle is not stolen. The patrol officer asks the driver for his license and registration. The driver claims that he does not have the vehicle registration, but he provides his driver's license to the patrol officer. The patrol officer asks the driver to wait while she checks his driver's license. **Using single-sign-on, the patrol officer queries the ISS and links to the state Department of Motor Vehicles (DMV) data repository to search for the driver's license number.** The DMV result shows that the driver's license number is invalid. In addition, **there is an officer notification alert from the ISS** stating, "Invalid driver's license numbers should be reported to Detective John Smith." The patrol officer arrests the driver for driving with an invalid license and contacts Detective Smith. Detective Smith requests that the patrol officer bring in the driver to establish identity and for further questioning relative to an active driver license forgery case.

Derived requirements from this scenario are shown in Table 3-6.

Table 3-6 Scenario 6 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Using single-sign-on, the patrol officer queries the ISS and links to the state Department of Motor Vehicles (DMV) data repository to search for the driver's license number	Functional	Patrol Officer
There is an officer notification alert from the ISS	Functional	System function

3.7 Scenario 7: Intelligence Analyst Officer Safety Alert

An intelligence analyst reviews tips and threats involving pen knife attacks on police officers. He **queries the regional ISS using the keywords "pen knife."** The **ISS returns incidents and cases that fit the inquired profile.** The analyst prepares an officer safety alert based on the ISS data detailing the pen knife attacks. The analyst's alert is passed on to Command Staff or his task force (if the analyst is supporting a multi-jurisdictional joint task force).

After receiving the alert, Command Staff **uses the ISS to disseminate the analyst's alert to all sworn staff and the multi-jurisdictional joint task force.** The task force uses the alert to strategize its next steps in tracking the specific, targeted criminal activity.

Derived requirements from this scenario are shown in Table 3-7.

Table 3-7 Scenario 7 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Queries the regional ISS using the keywords "pen knife"	Functional	Intelligence Analyst
ISS returns incidents and cases that fit the inquired profile	Functional	System function
Uses the ISS to disseminate the analyst's alert to all sworn staff and the multi-jurisdictional joint task force	Functional	Command Staff

3.8 Scenario 8: Officer Safety

A Call Center receives a 911 call and contacts Dispatch. The dispatcher alerts the nearest patrol units of the service call, and the nearest available patrol units respond to the call. Meanwhile, the dispatcher **queries the ISS for the history at the given address.** The **ISS returns known information about the address including the residents' names and possible children, any known felons, and any weapons or drugs data related to the address.** With the data retrieved from the ISS, the dispatcher alerts the en-route officers of any potential dangers at the reported scene. The officers take the appropriate cautionary actions when making their approach.

Derived requirements from this scenario are shown in Table 3-8.

Table 3-8 Scenario 8 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Queries the ISS for the history at a given address	Functional	Dispatcher
ISS returns known information about the address including the residents' names and possible children, any known felons, and any weapons or drugs data related to the address	Functional	System function

3.9 Scenario 9: Interface with Courts

Patrol officers respond to a dispatch call regarding a fight at a local nightclub. It turns out that no one is seriously injured and charges will not be brought against the individuals for their involvement in the fight. The patrol officers request identification from the individuals. One patrol officer uses **her wireless PDA to access the ISS** and **searches on the names of the individuals.** According to **court records available in the ISS** from a neighboring county, one of the individuals has a court-ordered restraining order against him and is not allowed in the county in which he has been found. The patrol officers take the individual to the local jail for violating the court order.

Derived requirements from this scenario are shown in Table 3-9.

Table 3-9 Scenario 9 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Uses her wireless PDA to access the ISS	Functional	Patrol Officer
Searches on the names of the individuals	Functional	Patrol Officer
Court records available in the ISS	Operational	System function

3.10 Scenario 10: Public/Community Outreach and Trust

The local police department maintains a community website that it uses to generate alerts, request help solving a case, or disseminate and receive general community information. **Tips and other information entered by the community are accessible only by law enforcement** and **made available in the ISS as appropriate.**

There is an unsolved armed robbery in a neighborhood. The police department asks the local media to broadcast the incident on the news, and agency staff posts a request for help solving the robbery on the police department community website. A man living in the neighborhood responds to the request with a tip (the tip is directly entered via the community website or is called in to be entered by agency staff). **The tip is then made available in the ISS.** The tip states that the man was out for a walk and saw an unknown woman with a dog tattoo walking through the neighborhood around the time the robbery occurred. He also provides a good description of the woman.

An investigator assigned to the armed robbery case, based upon the incident report provided by the victim, **searches the ISS using the keywords "dog tattoo." One of the results returned by the ISS is the man's tip with the physical description of the woman.** Based on all gathered information, a sketch is generated and posted to the community website to solicit more leads.

Derived requirements from this scenario are shown in Table 3-10.

Table 3-10 Scenario 10 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Tips and other information entered by the community are accessible only by law enforcement	Functional	System function
Tips and other information entered by the community are made available in the ISS as appropriate	Functional	Agency Staff
The tip is made available in the ISS	Operational	System function
Searches the ISS using the keywords "dog tattoo"	Functional	Investigator
One of the results returned by the ISS is the man's tip with the physical description of the woman	Functional	Investigator

3.11 Scenario 11: Photo Line-Up

A suspect has been arrested for cashing fraudulent checks at banks in the area. The suspect has been fingerprinted and a mug shot has been taken. **The arrest report information and the mug shot are made available in the ISS.**

The investigator assigned to the case is developing a photo line-up to determine if witnesses can identify the suspect. The investigator identifies physical features from observing the suspect and the mug shot. Physical features may include hair color, eye color, race, height, build, body markings, and scars. The investigator **logs into the ISS, enters the suspect's physical features as search criteria,** and **searches among mug shots entered into the ISS** by participating agencies across the region. The **ISS returns the suspect's mug shot and several photos, based on one or more of the physical features entered as search criteria.** The investigator selects the suspect's mug shot and a few photos resembling the suspect to compose an electronic photo line-up.

The **photo line-up is shown to witnesses**—bank tellers who have mistakenly cashed the checks for the suspect. Four of the five witnesses select the suspect from the photo line-up. This information is used by the prosecution in their case against the suspect, who has pled not guilty.

Derived requirements from this scenario are shown in Table 3-11.

Table 3-11 Scenario 11 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
The arrest report information and mug shots are made available in the ISS	Operational	System function
Logs into the ISS	Functional	Investigator
Enters the suspect's physical features into the ISS as search criteria	Functional	Investigator
Searches among mug shots in the ISS	Functional	Investigator
Mug shots entered into the ISS	Functional	Participating agencies across the region
ISS returns the suspect's mug shot and several photos, based on one or more of the physical features entered as search criteria	Functional	System function
Photo line-up is shown to witnesses	Functional	Investigator

3.12 Scenario 12: Phonetic Name Search

Officers are dispatched to a residential burglary in progress. Upon arrival, the officers see two individuals running from the residence. Officers confirm with the 911 caller, who is at the residence, that the two individuals are suspects in the burglary. One individual, Suspect A, is captured, but the other individual, Suspect B, escapes. Suspect A is arrested and questioned by an investigator. Suspect A tells the investigator that Suspect B is called "Billy" and believes he lives on or near "Gavlawn Avenue." The investigator **searches the ISS using the keywords "Billy" and "Gavlawn Avenue."** The **ISS returns a reference to a "Billie" in an incident report associated with another burglary in a neighboring county, along with his physical description and the contact information of the investigator assigned to the case.** The **ISS shows Billie's address as "Gavilan Avenue."** The physical description matches that of Suspect B. The investigator contacts the investigator assigned to the neighboring county case.

Derived requirements from this scenario are shown in Table 3-12.

Table 3-12 Scenario 12 Requirements Table

Derived Requirement	Requirement Type	Law Enforcement Role
Searches the ISS using the keywords "Billy" and "Gavlawn Avenue"	Functional	Investigator
ISS returns a reference to a "Billie" in an incident report associated with another burglary in the neighboring county, along with his physical description and contact information of the investigator assigned to the case	Functional	System function
ISS shows Billie's address as "Gavilan Avenue"	Functional	System function

This page intentionally left blank

4 Functional ISS Requirements

This section presents functional requirements based upon the best practices of established ISSs. These functional requirements are either fundamental or optional. Fundamental requirements are specifications of best practices that must be met to realize an effective ISS. These are stated as requirements that "must" be met. Optional requirements enhance ISS functionality, but are not essential when the ISS is first developed. These are stated as requirements that "should" be met.

Two key areas of ISS functionality are discussed in this section:

- System Architecture and Data Management
  - Common Architecture Requirements
  - Common Data Management Requirements
  - Additional Centralized/Hybrid Architecture and Data Management Requirements
  - Additional Distributed/Hybrid Architecture Requirements
- System Capabilities
  - Query
  - Outputs and Analytical Functions
  - System Administration

4.1 System Architecture and Data Management

The ISS architecture should meet the needs of the participating member agencies and their users. In adopting a particular architecture configuration, consideration should be given to the hardware and software legacy systems in place at the member agencies and the extent to which architectural implementation difficulty, cost, and manpower requirements will affect the ability to create an optimum ISS for those member agencies.

4.1.1 Common Architecture Requirements

Regardless of the technical architecture employed (see Section 2.1.2), there are common needs that form the basis for an effective ISS.

4.1.1.1 The ISS should be capable of interfacing to multiple external systems that provide information obtained by users via the ISS.

4.1.1.2 The ISS must have an architecture whereby the adding or removing of ISS components has minimal impact to the participating member agencies or their users and any other integrated data sources.

4.1.1.3 The ISS must integrate data sources to meet the interface requirements of the data sources.

4.1.1.4 The ISS must support configuration of external interfaces using commercially available standard interfaces.

4.1.1.5 The ISS must use a structured query language (SQL)-compliant database management system (DBMS).

4.1.1.6 The ISS must provide or support open database connectivity (ODBC) access to the DBMS.

4.1.1.7 The ISS must be implemented to have a graphical user interface (GUI) for accessing all functionality provided by the system.

4.1.1.8 Data transfers between an external system and the ISS should occur in an automated manner that does not require user intervention.

4.1.1.9 The ISS must execute functions to meet the initial design criteria for those functions.

4.1.1.10 The ISS must enable all functions to be performed via a GUI.

4.1.1.11 The GUI must be easy to use and require minimal training.

4.1.1.12 The GUI must employ intuitive navigation.

4.1.1.13 The GUI should provide forms for performing all ISS functions.

4.1.1.14 The GUI forms should have labeled data entry fields for the purpose of entering data for associated ISS functions.

4.1.1.15 The GUI form's data entry fields should enable data to be entered in a standardized format.

4.1.1.16 The GUI form's data entry fields should enable data to be entered using a standardized codes defined for the ISS.

4.1.1.17 Results from functions executed by the user should be displayed in a standardized format in the GUI.

4.1.1.18 Users should be able to print information displayed via the ISS GUI.

4.1.1.19 The ISS should support GUI screens capable of running on MDTs.

4.1.1.20 The ISS should support GUI screens capable of running on handheld PDAs.

4.1.1.21 The ISS's World Wide Web interface should enable ISS data to be accessed and displayed using a standard Internet browser over a secure connection.

4.1.1.22 The ISS Web-browser based application must impose minimal connectivity requirements on the client device.

4.1.1.23 The ISS must have a modular design.

4.1.1.24 The ISS should have a standardized platform for end-user client systems that facilitates the installation of system updates.

4.1.1.25 The ISS should be implemented using a Service-Oriented Architecture.

4.1.1.26 The ISS should enable access and use of the ISS by MDTs remotely connected to the network.

4.1.1.27 The ISS should enable access and use of the ISS by laptop computers remotely connected to the network.

4.1.1.28 The ISS should enable access and use of the ISS by wireless handheld devices (e.g., PDAs and cell phones) remotely connected to the network.

4.1.1.29 The ISS must support multiple types of communication services for remote device access.

4.1.1.30 The ISS must enable access and use of the ISS by workstations, desktops, and laptops directly connected to the network.

4.1.1.31 The ISS should provide a capability to support public access to a subset of ISS data and functions (e.g., a separate public web site).

4.1.1.32 The ISS must comply with a Global Justice Extensible Markup Language (GJXML) data model standard for exchanging data between the ISS and criminal justice data sources.

4.1.1.33 The ISS, where applicable, should provide users with a selection of external systems that can be accessed.

4.1.1.34 The ISS, where applicable, should notify the user when an external system is being accessed.

4.1.1.35 The ISS must comply with any applicable criminal justice privacy guidelines.

4.1.1.36 The ISS should comply with the NCISP guidelines.

4.1.1.37 Any ISS that shares intelligence data across jurisdictional boundaries must conform to the operation principles established by 28 Code of Federal Regulations (CFR) Part 23. (Data must meet the definition of "intelligence data" per the 28 CFR Part 23 for this to be applicable).

4.1.2 Common Data Management Requirements

One of the basic capabilities for an ISS is the ability to either store or provide access to a variety of data categories. The quality and precision of the data that is entered and maintained that is to be shared is the responsibility of the agencies who originate the data. Agencies have the responsibility for providing quality, accurate data to the ISS and for designating when that data is to be purged from the ISS. Agencies should conform to a common means of data representation. If they do not, users risk overlooking critical information due to a difference in terminology. The data that the participating agencies provide to the ISS should undergo consistent quality checks when being entered by agency personnel and be approved by their supervisors. Once the data is made available in the ISS, the data should not be modified in any manner by the system. The ISS must have an established method of maintaining the accuracy and currency of data accessed via the ISS. Depending on the ISS architecture, data is extracted from agency source RMSs and loaded into a centralized database and accessed from multiple agency and other data sources. Regardless of the architecture, ownership of the data remains the responsibility of the source agency.

The data managed by an ISS can be either fundamental or optional. Fundamental data categories are defined as those categories that meet minimum basic sharing needs of an ISS. Optional data categories add value to system use and to the efficiency of work processes among intended users. Some states may have restrictions on the extent to which some data may be shared. In some instances, the technology may not exist to electronically share the data.

4.1.2.1 An ISS must support the fundamental and optional data categories listed in Tables 4-1 and 4-2.
4.1.2.2 An ISS must protect all data so that it is accessible only to users with access authorization.
4.1.2.3 The ISS must not modify the data that is entered by participating agencies.
4.1.2.4 The ISS must ensure that agencies can update only the data that they originate.
4.1.2.5 The inclusion of data in the ISS must comply with all applicable rules and regulations.
4.1.2.6 The system should enable users to provide feedback pertaining to the ISS via the ISS.
4.1.2.7 Users should be able to enter success stories into the ISS.
4.1.2.8 Users should be able to enter comments on ISS use into the ISS.
4.1.2.9 Users should be able to enter responses to surveys about the ISS into the ISS.
4.1.2.10 The ISS should record user-provided feedback.

Table 4-1 Fundamental and Optional Shared Data Categories for External ISS Sources

Data Categories (External ISS Sources)	Fundamental	Optional
GIS Mapping Data		✓
Corrections Data		✓
Courts Data		✓
Criminal History Data	✓	
Critical Infrastructure Data		✓
Motor Vehicle Records		✓
Drug Data		✓
Probation and Parole Data		✓
Public Record Data (commercial fee services)		✓
Sex Offender Data	✓	
Local Warrants	✓	

Table 4-2 Fundamental and Optional Shared Data Categories for Internal ISS Sources

Data Categories (Internal ISS Sources)	Fundamental	Optional
Alerts/Lookouts/Be-On-The-Lookouts (BOLOs)	✓	
Arrest Data	✓	
Booking Data	✓	
CAD Incident Data	✓	
Evidence Data	✓	
Field Interview or Stop/Contact Data	✓	
Gang Data		✓
Incident Reports	✓	
Intelligence Data		✓
Investigative Case Data	✓	
Juvenile Data		✓
Mug Shots/Digital Photos	✓	
Narratives	✓	
Pawn Shop Data	✓	
Stolen Property Data	✓	
Traffic Citations	✓	

4.1.3 Additional Centralized/Hybrid Architecture and Data Management Requirements

The following are requirements for centralized and hybrid ISS configurations that differ from those for distributed configurations.

4.1.3.1 The ISS must have a defined common data structure or schema that can be used to map (transform) the elements in the data extracts from source data repositories to a common standard used in the ISS.

4.1.3.2 The ISS must have a common set of codes (e.g., vehicle type, hair color) that can be used to convert (transform) the codes in extracts from data sources to a common set used in the ISS.

4.1.3.3 The ISS should have a common geo-coding capability that can be used to convert (transform) addresses in extracts from data sources to common geo-coded addresses so that they can be used for mapping purposes.

4.1.3.4 The ISS must be capable of establishing a secure connection with systems that contain data sources for the ISS for the purpose of the initial load and subsequent updates of the centralized repository.

4.1.3.5 The ISS must provide the capability to extract, transform, and load (ETL) data from the data sources to the central repository for the initial load of the centralized repository.

4.1.3.6 The ETL must conform to the Interface Control Document (ICD) established for the ISS.

4.1.3.7 The ISS must provide the capability for periodic updating of the central repository with data from the data sources for maintaining the accuracy and currency of the centralized repository in synchronization with the data sources.

4.1.3.8 The ISS must provide the capability for data owners to selectively update data from their data source to the centralized repository.

4.1.3.9 The ISS must provide the capability for data owners to control when data will be transmitted from their data source to the centralized repository.

4.1.3.10 The ISS must provide the capability for a data owner to terminate transmission of any or all data from their data source to the centralized repository.

4.1.3.11 The ISS must provide the capability for the removal of all or selected data from the ISS database as required by the data owner.

4.1.3.12 Personal data loaded into the centralized repository should be de-conflicted on entry.

4.1.3.13 For data sources for which there is not an automated interface to the ISS, users must be able to enter data referred to in Tables 4-1 and 4-2.

4.1.4 Additional Distributed/Hybrid Architecture Requirements

The following are requirements for distributed configurations that differ from those for centralized and hybrid ISS configurations.

It is a common practice for owners of data sources to extract subsets of data from their RMSs and store them in separate repositories that are accessed by an ISS. The requirements below refer to these repositories as *distributed ISS repositories.*

4.1.4.1 The ISS should be able to access applicable data sources, such as local, regional, state, and federal law enforcement agency data sources, non-law enforcement agency data sources, and public record data sources.

4.1.4.2 The ISS must be capable of establishing a secure connection with systems that contain data sources for the ISS for the purpose of accessing distributed participating agency data sources and other data sources (e.g., DMV and public data sources).

4.1.4.3 The ISS should have the capability to use distributed ISS repositories of data that are dedicated ISS data sources maintained by the data owner (e.g., local agency).

4.1.4.4 For a distributed ISS repository, the ISS must support a common database schema that can be used to map data elements from a record data source to the repository.

4.1.4.5 For a distributed ISS repository, the ISS must support a common set of codes that can be used to convert data from a record data source to the repository.

4.1.4.6 For a distributed ISS repository, the ISS should have a common geo-coding capability that can be used to convert addresses from a record data source to common geo-coded addresses in the repository so that they can be used for mapping purposes.

4.1.4.7 For a distributed ISS repository, the ISS must provide the capability to enable the data owner to ETL data from the record data source to the repository.

4.1.4.8 The ETL must conform to the ICD established for the ISS.

4.1.4.9 For a distributed ISS repository, the ISS must provide the capability for the data owner to periodically update the repository with data from record sources for maintaining the accuracy and currency of the repository in synchronization with the record sources.

4.1.4.10 For a distributed ISS repository, the ISS must provide the capability for data owner to selectively update data from their data source to the repository

4.1.4.11 For a distributed ISS repository, the ISS must enable the data source owner to control when data will be transmitted to the repository.

4.1.4.12 For a distributed ISS repository, the ISS must enable the data owner to remove all or selected data from the repository.

4.1.4.13 For a distributed ISS repository, the ISS must provide the capability for the data owner to terminate transmission of any or all data from their ISS repository to the ISS.

4.1.4.14 For data sources that do not have an automated interface to the distributed ISS repository, users must be able to enter data referred to in Tables 13 and 14 into the repository.

4.1.4.15 The ISS must be able to recognize the status of distributed ISS repositories (e.g., local law enforcement agency data extract) and other data sources (e.g., DMV database).

4.1.4.16 The ISS must have the capability of displaying the status of distributed repositories and data sources to users that are using the system and are authorized access to that data source so that they are aware of which data sources may or may not be available.

4.1.4.17 The ISS must be capable of interfacing with other systems and data sources such as local, state, federal agency systems/data sources (e.g., NCIC and state employment commissions), as well as public record data sources.

4.2 System Capabilities

4.2.1 Query

Not all users will be able to access all information stored in the ISS. The term "query"—as it is used throughout this handbook—is defined as a request-response process.

Users should be able to retrieve data from the ISS via queries. Users should be able to query the ISS for information associated with a person, place, or thing (e.g., property and vehicles).

4.2.1.1 Users must be able to query the ISS for data, as designated in Tables 13 and 14.

4.2.1.2 Users must be able to query the ISS for data about a person.

4.2.1.3 Users must be able to query the ISS using a person's exact name.

4.2.1.4 Users must be able to query the ISS using a person's nickname.

4.2.1.5 Users must be able to query the ISS using a person's alias.

4.2.1.6 Users must be able to query the ISS using phonetic spelling of a person's name.

4.2.1.7 Users must be able to query the ISS using a person's attributes.

4.2.1.8 Users must be able to query the ISS for data about a place.

4.2.1.9 Users must be able to query the ISS using a place's exact location.

4.2.1.10 Users should be able to query the ISS using a geographic radius around a place.

4.2.1.11 Users must be able to query the ISS for data about a thing (e.g., property and vehicles).

4.2.1.12 Users must be able to query the ISS for associations.

4.2.1.13 Users must be able to query the ISS for aliases of associates.

4.2.1.14 Users must be able to query the ISS for the history of an address or location. History is defined as the set of events (incidents, arrests, etc.) that have occurred at the address or location.

4.2.1.15 Users must be able to request reports containing data returned by the ISS in response to user-initiated queries.

4.2.1.16 Users must be able to perform text searches.

4.2.1.17 The ISS must provide a phonetic search capability.

4.2.1.18 The ISS must provide a wildcard search capability.

4.2.1.19 Users must be able to perform single-character wildcard searches.

4.2.1.20 Users must be able to perform multiple-character wildcard searches.

4.2.1.21 The ISS must provide a capability to save results or a selected subset of results.

4.2.1.22 Users must be able to save search criteria.

4.2.1.23 Users must be able to retrieve saved search criteria.

4.2.1.24 Users must have the capability of resuming a search with saved search criteria.

4.2.1.25 Users must be able to search by ranges on a person's attributes (height, weight, age, etc.).

4.2.1.26 The ISS must have a GoogleTM-like text-search capability.

4.2.1.27 The ISS must be capable of producing the same set of query results if the data in the ISS and the query parameters have not changed.

4.2.1.28 The ISS should enable users to query the ISS for user feedback that has been previously entered by users.

4.2.1.29 Users should be able to request recorded success stories.

4.2.1.30 Users should be able to request recorded comments on ISS use.

4.2.1.31 Users should be able to request recorded responses to surveys about the ISS.

4.2.1.32 Users should be able to view user feedback that has been previously entered by users.

4.2.2 Outputs and Analytical Functions

One of the major advantages for law enforcement agencies participating in an ISS is the ability to obtain consolidated outputs and perform analysis on regional data sets. Law enforcement agencies know that criminals do not respect jurisdictional boundaries and tend to perpetrate a wave of crime across an entire area. The ISS provides analysts with a comprehensive view of crime to gain insight on where future problem areas could occur, which areas to tactically focus on, and other patterns that could reveal where suspects live or operate.

4.2.2.1 The ISS must provide a print capability for data returned by the ISS.

4.2.2.2 Users must be able to initiate the ISS print capability.

4.2.2.3 The ISS must be able to label each page that is printed with the appropriate text describing how the data can be distributed, including any distribution restrictions or other disclaimers, as appropriate.

4.2.2.4 The ISS must generate user-requested reports.

4.2.2.5 In response to a query, the ISS must return along with hits (responses matching the query request) the original parameters entered as search criteria.

4.2.2.6 The ISS must provide a link association capability that provides users with information pertaining to associations among people, places, and things that have been established among recorded data elements.

4.2.2.7 Users should be able to create associations among people, places, and things in the ISS.

4.2.2.8 The ISS should provide a link analysis charting capability for crime analysis.

4.2.2.9 The ISS should provide a mapping capability to display specific locations and regions of interest.

4.2.2.10 The ISS mapping capability should display geographical locations of recorded data elements.

4.2.2.11 The ISS mapping capability should display established associations among people, places, and things.

4.2.2.12 The ISS should provide a notification capability to alert users of critical information associated with a person or location (e.g., officer safety notifications and business area crime notifications).

4.2.2.13 The ISS should provide an electronic photograph lineup capability.

4.2.2.14 The ISS should provide the capability to return information based on protection assigned to the data: complete information, minimal information with point of contact, no information with a notification to data owner.

4.2.2.15 The ISS should not leave information from a user's session displayed after the user has logged off.

4.2.3 System Administration

System administrators authorize users to access the system, and each user is granted specific data access rights based on their defined roles in the law enforcement agency or ISS organization. A common practice is to devise a scheme so that usernames are never deleted or reissued to another user. This practice preserves account uniqueness and historical audit report integrity.

System administrators should be able to establish operational parameters for creating audit logs to capture and record system performance and users' access to data in the ISS. System administrators should also be able to search and print these logs in report format. For the following requirements, the term "administrators" refers to authorized agency system and security administrators.

4.2.3.1 The ISS must provide a capability for the system administrator to distribute system messages, updates, and releases.

4.2.3.2 The ISS should provide a capability for the system administrator to push applications from one centralized location to one or more end-user devices.

4.2.3.3 The ISS must provide the capability for system administrators to administer usernames and passwords.

4.2.3.4 The ISS must provide the capability for system administrators to create and activate a user account.

4.2.3.5 The ISS must provide the capability for system administrators to deactivate and reactivate a user account.

4.2.3.6 The ISS must provide the capability for system administrators to modify access rights for user accounts.

4.2.3.7 The ISS must provide the capability for system administrators to deactivate specific device access to the system (e.g., an end-user device).

4.2.3.8 The ISS must provide the capability for system administrators to activate and deactivate functions in the ISS (e.g., deactivated function should not be accessible).

4.2.3.9 The ISS must have the capability for system administrators to activate and deactivate access to selected data in the ISS by the ISS system administrator (e.g., agency leaves ISS and its data must be removed).

4.2.3.10 The ISS must provide a capability for system administrators to specify access controls, based on user and group identification for all system components (programs, files, transactions, system screens, and devices).

4.2.3.11 The ISS must provide a capability for system administrators to control access for users and groups to select sensitive fields of applications (e.g., victims' names, juvenile records).

4.2.3.12 The ISS must provide a capability for system administrators control access for users and groups to select screens of the applications.

4.2.3.13 The ISS should enable a system administrator to perform any defined system task from any authorized workstation.

4.2.3.14 The ISS should enable a system administrator to print system-related information to any printer within the authorized ISS network.

4.2.3.15 The ISS must provide for date and time stamps in the audit log for all administrative tasks.

4.2.3.16 The ISS must provide a capability for system administrators to control access users and groups to select functions (e.g., reports, configurations, and activities).

4.2.3.17 The ISS must document user activity (who and what) in an audit log for use by system administrators for traceability—ensuring approved use of the system by users.

4.2.3.18 The audit log must contain the unique user identity for user-triggered events.

4.2.3.19 The ISS must contain date and time stamps for all entries in the audit log.

4.2.3.20 The audit log must record events triggered by users including data created, deleted, and modified by users.

4.2.3.21 The audit log should contain the network address of the connection for all authentication events.

4.2.3.22 The audit log should contain details of any successful access to controlled information.

4.2.3.23 The audit log should contain details of any unsuccessful access to sensitive information.

4.2.3.24 The ISS must provide mechanisms to protect the audit logs from unauthorized access.

4.2.3.25 The ISS must provide mechanisms to protect the audit logs from unauthorized modification.

4.2.3.26 The ISS must provide mechanisms to protect the audit logs from unauthorized destruction.

4.2.3.27 The ISS must display a warning message if an attempt is made to delete a user account or reissue an existing account to another user and document the action in the audit log.

4.2.3.28 The ISS must provide a capability that enables system administrators to query results in the audit log(s).

4.2.3.29 The ISS must provide a capability that enables system administrators to search an audit log based on one or more of the following parameters: time range, before or after a specific time, by type of transaction, by username, by user group.

4.2.3.30 The ISS should provide a capability that enables system administrators to generate both detailed and summary reports of audit results for selected audit information (e.g., audit information for one user).

4.2.3.31 The ISS must be able to capture operating statistics in a system log for use by system administrators for managing system performance.

4.2.3.32 The ISS should log productivity statistics in a system log for measuring individual user and group use of the system.

4.2.3.33 The ISS must provide a capability that enables system administrators to query the system log of operating statistics and create reports.

4.2.3.34 The ISS must contain data and time stamps for all entries in the system log.

4.2.3.35 The ISS must capture the number of users accessing the ISS at any given time.

This page intentionally left blank

5 Operational ISS Requirements

Operating an ISS involves the operation and management of the system to ensure authorized users are accessing the ISS appropriate to their role(s) and to ensure agency data is being managed according to the security policies and procedures established. It also involves providing capabilities to determine whether the ISS is providing a true value to system end users. Traditional forms of performance gauges such as throughput and response time, reliability, availability, and scalability must also be included. Also addressed must be maintenance, disaster recovery, and providing continuity of operations (COOP). Last, providing initial and refresher training to ISS end users becomes an ongoing process with an ISS program that should not be overlooked. ISS requirements supporting these operational capabilities are described further in the following subsections:

- User Authentication, Authorization, and Access
- Security
- System Performance
  - Metrics Collection
  - Throughput and Response Time
  - Availability
  - Scalability
- System Support
  - Maintenance
  - Backup and Recovery
  - COOP/Survivability
- Training

5.1 User Authentication, Authorization, and Access

The ISS must meet user authentication, authorization, and access requirements as set forth in security policies and procedures developed by ISS management/governance. The following requirements, which are considered a minimum set, establish the criteria for authenticating a user to an ISS and are specific to the type of ISS configuration or architecture referenced. User authentication and authorization is an important function for an ISS that involves ensuring a user attempting to access the system is a unique person with authorized ownership of the user account. In most ISSs, usernames and passwords are the primary method used to gain access to the system over a secure communications network. Other controls limit access to specific workstations, ports or work locations. However, more robust methods of user authentication—such as biometric-based authentication methods—are expected to become more prevalent in the coming years.

There are two primary methods for access control—federated and centralized. Federated identity technologies provide a means to link local agency users to an external ISS application, without the burden of managing their identity and credential information in both places. This is accomplished by establishing a trusted relationship among the applications thus allowing the user to have a single sign-on capability. Under a centralized model, identity is controlled via the central ISS but permissions or rights can be managed either centrally or by the individual agencies.

Under each model, in addition to law enforcement users, some ISSs provide access to subsets of ISS information to the public. For example, a public ISS website can provide information about crime and public safety in the region.

Regardless of the model, those involved with ISS management/governance are strongly encouraged to review the guidance provided in the NIST publications referenced in the Appendix. These publications, which are referred to in several of the requirements in this and following sections, provide specific guidelines for securing information technology systems.

5.1.1 The ISS should provide authentication measures that are compliant with NIST 800-14, 3.11.2

5.1.2 The ISS must authenticate users using a unique username and password.

5.1.3 The ISS must have username and password complexity that meets security requirements per ISS security policies and procedures (e.g., minimum password length, non-trivial passwords).

5.1.4 The ISS must have password maintenance capabilities that meet security requirements per ISS security policies and procedures (e.g., password initialization, password reset, password expiration notice).

5.1.5 The ISS must display a legal notification at logon that informs the user that the system is a law enforcement system.

5.1.6 The ISS must display a legal notification at logon that informs the user that all user transactions are logged.

5.1.7 The ISS must support either a Federated or Centralized method to manage user authentication, authorization and access.

5.1.8 The ISS should provide capability to disable a user's account after multiple login failures, per the ISS security policies and procedures.

5.1.9 The ISS should provide mechanisms to restrict access by workstation, port, or address.

5.1.10 The ISS should support token-based authentication.

5.1.11 The ISS should support biometrics-based authentication.

5.1.12 The ISS should support logical access controls as specified in NIST 800-14, 3.12.1.

5.1.13 The ISS must provide the capability for each agency to determine the access privileges of its users and groups.

5.1.14 The ISS should provide a capability to manage access privileges for users, groups, and roles.

5.1.15 The ISS must have the capability to define a system administrator user role for managing the ISS.

5.1.16 The ISS should have the capability to define a public user role for accessing a subset of data and functions designed for public use.

5.1.17 The ISS must provide the capability to create user groups.

5.1.18 The ISS must determine the level of access authorization for the user.

5.1.19 The ISS must determine the level of access authorization for a group.

5.1.20 The ISS should transmit the user's level of access authorization information to subsystems as they are accessed by the user.

5.1.21 The ISS must have the capability to assign roles to users and groups.

5.1.22 The ISS must have the capability to assign multiple roles for a single user.

5.1.23 The ISS must have the capability to assign access privileges to data available in the ISS (e.g., by username, agency, role).

5.1.24 The ISS must have the capability to assign access privileges to functions (e.g., enter, delete, query, reports) available in the ISS (e.g., by username, agency, role).

5.1.25 The ISS must have the capability to restrict access privileges to data available in the ISS (e.g., by username, agency, role).

5.1.26 The ISS must have the capability to restrict access privileges to functions available in the ISS (e.g., by username, agency, role).

5.1.27 The ISS must provide a capability for an agency to restrict access to data (e.g., juvenile data) supplied by that agency (e.g., by username, agency, role).

5.1.28 The ISS should provide the capability for an agency to restrict its data with respect to user location (e.g., remote access could be prohibited).

5.2 Security

The ISS must also meet security requirements as set forth in security policies and procedures developed by ISS management/governance. These requirements provide measures for protecting the system from unauthorized access and protecting the integrity of the data, functions, and components. The following requirements are considered a minimum set. Those involved with ISS management/governance are strongly encouraged to review the guidance provided in the NIST publications referenced in the Appendix. These publications provide specific guidelines for securing information technology systems.

5.2.1 The ISS must be operated in a facility(s) that is (are) certified for storage of law enforcement Sensitive But Unclassified (SBU) data.

5.2.2 The ISS must provide the capabilities and integrating components in a secure manner as directed by ISS security policies and procedures.

5.2.3 The ISS must support Secure Socket Layer (SSL) encrypted connections.

5.2.4 Thee ISS must support secure virtual private network connections.

5.2.5 The ISS must protect ISS software from unauthorized, accidental, or malicious modification or destruction.

5.2.6 The ISS must protect ISS application data unauthorized, accidental, or malicious modification or destruction.

5.2.7 The ISS must provide a means to detect unauthorized access of the ISS (e.g., to its data, functions, and components).

5.2.8 The ISS must provide the capability for all components to have virus protection and maintain it.

5.2.9 The ISS should provide a capability to install and maintain virus protection from one centralized location to end-user devices.

5.2.10 The ISS must provide deactivation of user access without requiring a shutdown of the system software or operating system.

5.2.11 The ISS should provide a means to restrict access to specific functions from a specific terminal or network device.

5.2.12 The ISS should provide a means to expire a user’s access rights (e.g., temporary users of a task force).

5.2.13 The ISS should provide the capability to provide real-time alerts for critical events (e.g., intrusion detection, power outages).

5.2.14 The ISS should provide the capability to provide selected real-time alerts to end-user mobile devices, such as pagers and cell phones.

5.2.15 The ISS should provide secure access for authorized users to use the system.

5.2.16 The ISS should ensure that a function enacted by a user comes from an approved location within the region.

5.3 System Performance

ISS governance/management is responsible for determining performance goals for the ISS. The performance of the system can be measured by cataloging, capturing, and evaluating metrics of the system’s transactions with respect to user interaction with the system and the system’s responses. A needs analysis may be conducted during the planning phase—with follow-on analysis—to determine whether performance requirements are being met.

The requirements listed below outline the areas of consideration for assessing system performance. [Note: Specific performance measures and expected values are beyond the scope of this document.]

5.3.1 Metrics Collection

Metrics may be in the form of transactions tagged by the ISS, user feedback (surveys), or agency or ISS governance/management input on program operations. There are two primary categories of metrics that should be collected—metrics for assessing ISS performance and metrics for assessing impact of the ISS on day-to-day operations. Section 7 provides a discussion on a methodology for metrics collection and recommendations on specific types of metrics to collect. High-level requirements to allow for the collection of metrics are listed below.

5.3.1.1 The ISS must meet the initial metrics design goals.

5.3.1.2 The ISS must be capable of automatically capturing data that has been designated as necessary in the initial design goals for evaluating whether the system is meeting its goals and objectives (e.g., functions used and concurrent number of users).

5.3.1.3 The ISS should enable users to enter designated metrics via a GUI.

5.3.1.4 The ISS must enable designated users to retrieve and review metrics data.

5.3.1.5 The ISS should have a capability to compile and retrieve selected metrics that can be used for analysis and report generation.

5.3.1.6 The ISS should have the capability to capture and compile the number of users accessing the system during a designated time period.

5.3.1.7 The ISS should have the capability to capture and compile results of the number of system functions executed by type, processed during the pre-specified period.

5.3.1.8 The ISS should have the capability to capture data that can be used to measure system response times for function execution.

5.3.1.9 The ISS response time should be measured from the time a function or system operation is initiated by a user until the start of the information display on a user's screen.

5.3.1.10 The ISS should capture the types and related number of functions executed.

5.3.1.11 The ISS should determine the total number of users that can be connected to the system at any one time.

5.3.2 Throughput and Response Time

ISS governance/management is responsible for determining initial design goals in terms of specific operational capabilities of the ISS. For example, there may be a design goal that sets an expected response time under various conditions and types of query used. This measure has a significant impact on the amount of hardware needed for the ISS.

5.3.2.1 The ISS must meet the initial throughput and response times design goals.

5.3.2.2 The ISS must meet the initial design estimate of the number of users that will access the system during the pre-specified time period.

5.3.2.3 The ISS must meet the initial design estimate for the number of system functions executed by type and per the pre-specified time interval.

5.3.2.4 The ISS must meet the initial design estimate of the number of multiple data source that will be accessed.

5.3.2.5 The ISS must meet the initial design estimate for executing system administrative functions.

5.3.2.6 The data owners must be able to perform database maintenance on their ISS data sources without causing system degradation.

5.3.2.7 The ISS must meet the initial design estimates for peak periods of system use.

5.3.3 Availability

Availability is an important consideration when designing an ISS. It is important to understand the intended operational use of the system. Is the ISS considered a mission-critical system, like an RMS, or is it only a support system? High availability generally means much higher hardware and software costs. High availability also implies COOP and other automatic fail-over mechanisms will be established.

The following requirements establish the criteria for the availability of the ISS.

5.3.3.1 The ISS must meet the initial availability design goals.

5.3.3.2 The ISS must meet the initial availability design goals. For example, an ISS could provide system availability (as defined in Appendix A) of 98 percent and the ISS should not sustain a system downtime period (as defined in Appendix A) in excess of 10 minutes.

5.3.3.3 The system must be available 24 hours a day, 7 days a week. The system is considered unavailable any time it does not fully meet the functional and performance requirements specified in the design goals, whether due to failure or preventive maintenance.

5.3.3.4 The ISS should support continuous operation without user intervention in the event of a single component failure.

5.3.3.5 The ISS should be fault tolerant to accommodate minor interruptions in subsystems without causing unavailability.

5.3.4 Scalability

As with availability, scalability also has an impact on system costs. It is essential that system growth forecasts be taken into consideration at initial deployment to ensure that sufficient hardware, software, space, power, and other resources can be added to meet future needs.

5.3.4.1 The data sources that are part of the ISS should be scalable per design goals (e.g., the amount of data can increase with the addition of participating agencies and agency growth).

5.3.4.2 The data sources that are part of the ISS should be capable of incorporating additional data element types.

5.3.4.3 The ISS must provide sufficient storage for expansion of log files per design goals.

5.3.4.4 The ISS should provide capability to archive logs files in a way that does not exceed the expansion design goal for log files.

5.3.4.5 The ISS should be capable of supporting the total number of concurrent users per design goals (e.g., support for current and planned expansion of software licenses).

5.3.4.6 The ISS network connectivity (bandwidth) should be scalable per design goals.

5.3.4.7 The ISS should ensure that the number of users does not exceed the allowable number for each user license type.

5.3.4.8 The ISS number of executed functions should be scalable per design goals.

5.3.4.9 The ISS system response time should be scalable per design goals.

5.3.4.10 The ISS system availability should be scalable per design goals.

5.4 System Support

The following requirements establish the criteria for operating and maintaining the ISS hardware and software components. At a minimum, the ISS shall include a development environment (DE) and test environment (TE) separate from the production environment (PE).

5.4.1 Maintenance

System administrators should be able to perform routine maintenance with minimal disruptions to the operational performance of the ISS.

5.4.1.1 The ISS should be capable of replacing failed hardware components with spare hardware components within a pre-specified time period.

5.4.1.2 The ISS should be capable of replacing (reloading and rebooting) failed software components within a pre-specified time period.

5.4.1.3 The ISS should ensure that hardware updates are installed without disruption of service to member agencies or users.

5.4.1.4 The ISS should ensure that software updates are installed without disruption of service to member agencies or users.

5.4.1.5 The ISS should incorporate Service Level Agreements (SLAs) with vendors to set levels of system performance and tiered problem response plans.

5.4.2 Backup and Recovery

System administrators should perform backup and recovery operations for ISS hardware and software system components on a regular basis or as a result of operational system failures. The backup and recovery operations should ensure that the system is returned to its last fully operational state, including the most recent instance of the data repository.

5.4.2.1 The ISS should provide a capability to perform recovery of system hardware components.

5.4.2.2 The ISS should provide a capability to perform recovery of system software components.

5.4.2.3 The ISS should provide a capability to perform recovery of system data.

5.4.2.4 The ISS should provide a capability to perform automatic backup of system data.

5.4.2.5 The ISS should provide a capability to perform a backup of a centralized data repository, if applicable.

5.4.2.6 The ISS should incorporate at minimum a cold backup location that stores archived copies of the data in the event of a catastrophic failure of the primary ISS site. A cold backup location only stores off-line copies of the ISS data and applications.

5.4.2.7 The ISS should have a backup and recovery plan that specifies the procedures for restoring the ISS operations, emergency contact information, and scheduled testing of the backup procedures.

5.4.3 COOP/Survivability

The following requirements establish the criteria for providing a COOP capability in the event of a major disruption to an operational site.

5.4.3.1 The ISS should employ a backup system capability to maintain adequate survivability in the event of a critical disturbance to system operations.

5.4.3.2 The ISS should establish a COOP site to host the backup system.

5.4.3.3 The ISS should enable user connectivity to the COOP site backup system, if necessary.

5.4.3.4 The ISS should be capable of replicating the most recent centralized data repository at the COOP site, if necessary.

5.4.4 Training

Training requirements and training program content should be determined by the ISS program management or governance body, consistent with ISS program policies and procedures. Training of authorized ISS users should be provided prior to granting first-time users access to the system.

Two ongoing components of any program are user feedback and on-line help support. These two components augment training and provide immediate options for users to provide information to enhance the training program, as well as obtain help support.

5.4.4.1 The ISS should enable users to provide user feedback, such as success stories, comments, or suggestions regarding the ISS. For example, success stories can exemplify how the ISS can be used to close cases, generate leads, or otherwise further investigations.

5.4.4.2 The ISS should prompt the user to enter user feedback.

5.4.4.3 The ISS should prompt the user to enter success stories at predefined points in the user's work process.

5.4.4.4 The ISS should make a comment/suggestion box/link available to the user to enter comments and suggestions at predefined points in the user's ISS session.

5.4.4.5 The ISS should prompt the user to enter responses to surveys made available on the ISS.

5.4.4.6 The ISS should enable any authorized user to access user feedback entered by other users.

5.4.4.7 The system should provide an on-line help system.

5.4.4.8 The ISS should provide the capability for an on-line training module that explains all system functions and rules.

5.4.4.9 The ISS should be able to update the training module contents from formatted screens.

5.4.4.10 The ISS should support computer-based training (CBT) for use by both data contributors and users of the ISS, to be placed on the ISS network in downloadable formats.

This page intentionally left blank

6 ISS Program Organization: Considerations for Implementing an ISS

This section is provided for practitioners who are considering implementing or joining an ISS. Topics are separated into programmatic and technical considerations. The purpose of this information is to share guidance from ISSs on how to create an environment that facilitates effective information-sharing. Such an environment is necessary to ensure that the implementation of ISS functional and operational requirements results in a successful ISS.

6.1 Programmatic Considerations

As law enforcement agencies shift their focus from local to regional crime prevention, the need arises for better knowledge of the programmatic concerns associated with the implementation of a successful ISS. These programmatic considerations include governance, management, policy, and funding.

6.1.1 Governance

Typically, a governance organization or consortium is formed when agencies want to initiate an ISS program and doing so is beyond the capabilities of a single agency. However, a governance entity may not be necessary when there is a single agency or organization with overall management authority for the regional system. This is the model that CLEAR has employed. Though a single organization has management authority, this does not imply that close coordination with participating agencies is not necessary. Now that CLEAR is being expanded to a statewide system, the need for a formal governance entity has been recognized.

The governance organization is a shared management approach that enables participating agencies to effectively collaborate. The primary purpose of a governance organization is to have a formal entity that has the authority and responsibility for overseeing the ISS program on behalf of all participating agencies. Successful governance organizations have representatives from each member agency that are the key decision makers for the agency such as chiefs and sheriffs. The responsibilities of the governance organization include the following:

- Establishing policies and procedures, especially a memorandum of understanding (MOU)
- Defining strategic goals for the ISS that support individual agency and regional business needs
- Putting in place and overseeing a management team for the ISS
- Developing requirements for the ISS that meet strategic goals and user needs
- Obtaining and managing funding for development and operations
- Promoting the ISS and demonstrating effectiveness

Policies and Procedures

Developing an MOU for the ISS should be one of the first actions for the Governance Board. The MOU outlines the policies that govern the activities of the agencies, including the roles and responsibilities of all persons who interact with the ISS. It also documents the mission, goals, and objectives of the ISS. The MOU is also a legal document that each agency signs. It is reviewed by agency legal authorities and signed by each agency. All ISSs have found that obtaining MOU signatures is time-consuming; therefore, the MOU should be as simple and straightforward as possible.

The Governance Board also reviews and approves multiple policies and procedures developed by management. These policies and procedures are further discussed under Section 6.1.2 Management.

Roles and Responsibilities

The Governance Board also should create rules regarding membership. Participants in the governance organization can include voting members and non-voting members. Each voting member has one vote. Once an ISS is established, member agencies vote to allow additional agencies to join the ISS. Agencies can withdraw at any time from the ISS and when this occurs, their data is removed from the ISS. Agency membership can also be terminated if the agency violates the terms of the MOU that the agency signed. Non-voting members may represent those who do not provide data to the ISS but have a stake in its success. Typical non-voting members can include public safety agency representatives, federal agency representatives, non-member law enforcement agency representatives, and persons holding office at the local, state, and federal level.

A board of directors is established, and committees are formed to work on specific issues. Committees are typically formed to address technical and other programmatic issues that arise that require separate analysis and discussion. Committees then provide one or more recommendations to the governance board. Commonly, governance organizations have a Business or Policy Committee that works on defining the business needs and a Technical Committee that makes implementation and operational recommendations. Users and technical representatives participate in committees that develop requirements. For a new ISS, an RFP may be developed that would include functional and operational requirements. The Governance Board will have to decide such matters as the initial operating capabilities of the proposed system, the number of agencies to be connected, and the number of users to be served.

Coordination Though Regular Meetings

Governance or Board meetings should be held monthly or bi-monthly. In some ISS programs, the meetings are open to the public. This approach promotes communication among member agencies and enables discussion of ISS status and recommendations for any necessary actions. Committees meet as necessary to work on their assigned issues. Minutes of the Governance Board meetings are captured and circulated to stakeholders; in some instances, they are available to the public as well. Likewise, minutes of committee meetings are sometimes documented and circulated.

ISS Promotion

Successful ISSs have an individual who is an advocate for the system and is instrumental in influencing agencies to join and provide data to the ISS. In some instances, that individual or another key person is very successful in obtaining grant funding for the development of system capabilities. More mature ISSs have found that it is necessary to “market” the system to its intended users. Management personnel within participating agencies are kept informed on a regular basis of plans and of any impending dates for new capabilities to become operational. Supervisors are expected to inform their subordinates, thereby creating interest in the program and establishing an environment that encourages system use. The Governance Board must substantiate the effectiveness of the ISS to senior management in stakeholder agencies and to potential funding sources. The management team is typically responsible for developing the basis for substantiating the ISS’s effectiveness.

6.1.2 Management

The management team is established by the governance organization. The governance organization provides the funds necessary to hire or contract individuals for the management team. The management team works at the discretion of the Governance Board. Management team responsibilities can be broad and include the following:

- Develop and submit an ISS program budget to the Governance Board
- Establish and annually review the policies and procedures developed for the ISS
- Work with Technical/User Committees and vendors to schedule and carry out the design and implementation of system capabilities
- Oversee the daily operation and maintenance of the system hardware and the system and application software
- Obtain and maintain contracts with hardware, software, system developer, and system integrator vendors
- Direct vendor personnel
- Develop and operate training programs
- Develop and operate a 24x7 help desk capability

- Collect and analyze data on the effectiveness of the ISS
- Coordinate the signing of the MOU by agencies that want to join the ISS
- Oversee the hardware, software, and data integration necessary for adding an agency's data to the system and providing access for its users
- Coordinate with legal staff and privacy experts
- Report status to the Governance Board periodically

Several of these responsibilities are further discussed below.

Policies and Procedures

Management typically is given oversight on all policies and procedures for the ISS program and can be instrumental in their initial development. For example, a separate Security Policy and Security Agreement are typically developed. The purpose of the Security Policy is to consolidate the security requirements of individual agencies into one cohesive policy for the ISS program. It contains details on all the security aspects of the ISS.

Most ISS users are required to sign a Security Agreement prior to being given access to the system, typically after completing training. This agreement details the responsibilities for using the ISS and explains restrictions under which data from the ISS can be used. For example, all ISSs, because they are not systems of record, require users to validate information with the originating agency.

The security policy also defines how information printed from the system that contains sensitive information should be labeled. For example, security markings can include the name of the user printing the material, date and time printed, and level of security.
Most ISSs and some vendors have recently engaged privacy experts to help develop a privacy policy for the ISS. The privacy policy ensures that the functionality provided by the system meets privacy regulations and is defensible should questions or objections be raised by privacy advocates. The privacy policy should also be reviewed with new users during training.

A common practice is for Management to review the MOU, security agreement, and privacy and security policies annually and revise them as needed based on current ISS objectives.

ISS Program Evaluation

One of the key functions of the management team is to develop justification for the continued funding and operation of the ISS. Typically, ISS user feedback is solicited for this purpose. Users are strongly encouraged to provide success stories. Some ISSs are beginning to implement metrics programs and automatically collect data that can be used to demonstrate that the system is effective. All ISSs have faced the problem of demonstrating effectiveness; as yet, none have established an ISS program evaluation capability.

Effective Training Programs

The importance of providing effective training in use of the ISS should be recognized by those considering an ISS program. Despite the fact that the emphasis continues to be on new system development and operations in many ISSs, the interview results confirmed the need for better training programs. Although the length of user training and types of training materials employed varied among the ISS organizations, three training approaches emerged from the interview results.

- **Direct Training:** The most effective training requires trainees to attend a dedicated training session with an opportunity for hands-on practice. The training facility has a workstation for each student. There is one trainer, a sworn officer, and an assistant who is available to help anyone having difficulty keeping up with the class.

The direct-training method reaches the greatest number of users with the most consistent presentation of the ISS application. Training ranges from a half day to a full day.

- **Train-the-Trainer:** Another training model commonly used is a train-the-trainer approach. Representatives from each participating agency receive the classroom training, which they then take back to the field and share with other officers. While the trainer serves as an advocate for the new system in the field, each trainer may vary in the amount of material absorbed and perspective of the new system.
- **Intuitive Design/Mentoring:** This approach assumes that the design of the system is so intuitive that no formal training is necessary. Many times, these systems contain a robust set of help screens. Regular day-to-day use is supplemented by system mentors (experts)—
essentially on-the-job training. This technique is most effective for users that repetitively access a specific set of features or functions.

Figure 6-1 shows the relative percentages of surveyed organizations using each training approach.

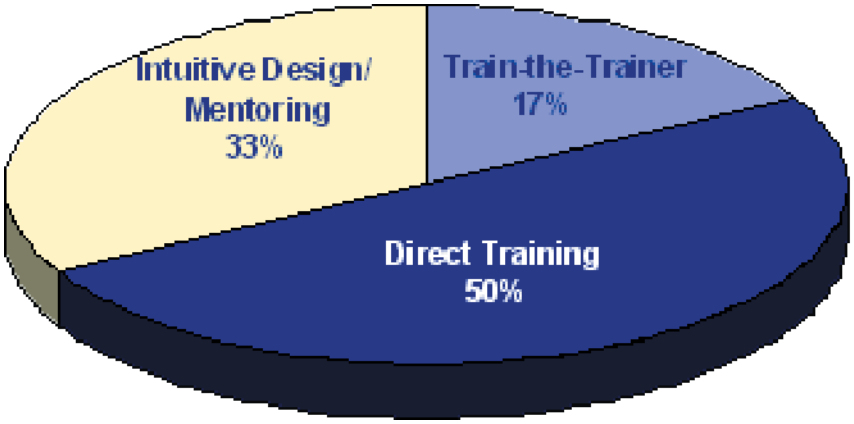

Figure 6-1 ISS Training Approaches

24x7 Help Desk Support

Help desk support is another difficult and expensive capability to provide effectively. Since help desk support needs to be available 24x7, the staffing requirements can be expensive. Extra staff is needed to cover for individuals when they are on leave. In addition, for an effective Help Desk, members need time to collaborate and share methods they may individually devise to solve problems. It is also typical that users prefer to contact someone in their agency for help first. A common practice is to have a person in each division as the point of contact for assistance within the agency. That person is usually a “power user” and is typically very proficient in using the system. Problems can be escalated to the ISS Help Desk as necessary. Although on-line help is available in most ISSs, patrol officers, in particular, seem to not use on-line help frequently. Officers prefer to contact someone they know for help.

Effective Development Practices

The use of standard documentation practices during ISS development is another consideration that contributes to successful ISS development. Most ISSs do not follow rigorous software development methodologies since doing so can be very expensive. However, producing standardized documentation during the design and development phases provides a baseline for consistent development practices among different development teams over the evolution of the system. This ensures a minimum level of consistency is established and is crucial when there is design/development staff turnover during subsequent implementation phases.

Other common success factors are that the development process is typically iterative. This enables an initial capability to be deployed with subsequent capability added as time and funding allows.   It also enables users to become proficient on a smaller set of features and then build on their skills as new features are added, which promotes user acceptance.

Another development practice is establishing separate development, training, and operational system/database environments. This practice allows the operational components to be dedicated for operational use.

During the design process, it is important that the management team can call upon legal staff to discuss any potential legal impacts of requirements that are being recommended for development. This is a proactive way of avoiding potential serious legal issues, and software modification costs, after the system is deployed.

Another effective practice is to allow end users to participate in the development of requirements and testing. Frequently, a new release or new capability is field-tested by a small number of users or "beta-test" groups, before being released ISS-wide.

Finally, new software releases should be placed into operation with sufficient capacity to handle a much larger number of users than would normally be expected to use the new capabilities. Once users have investigated the new capabilities, usage typically drops and the components providing the extra capacity can be redeployed. New releases are placed into operation early in the workweek when there is ample opportunity for the development staff to do a roll-back should it be necessary.

6.1.3 Public Access

One capability that should be considered, though not typically considered feasible for an initial ISS implementation, is providing a public web site. The web site can be used for access to certain ISS applications and data. For example, more mature ISSs have created web sites that allow the public to display crime maps in selected neighborhoods and provide crime statistics. Web sites are also useful for dissemination of information (e.g., wanted persons). An additional feature that has been implemented is business notifications. Businesses can be notified of emerging regional crime patterns, including notifications that request a business's support (e.g., turn on business-owned surveillance cameras) to proactively address criminal activity that may emerge in a particular area.

6.1.4 Funding

ISS management, with support from the governance body, is also responsible for obtaining sufficient funds to sustain the costs associated with ISS development, operation, maintenance, enhancement, and management overhead. Individuals participating on the Governance Board or management team are typically not paid by the ISS for their participation.

Funding Sources

Most ISSs have been established with funding obtained from grant sources. Many rely on grant funds to pursue enhancements. There is a common need for reliable yearly renewal of funding to sustain maintenance agreements, licenses for hardware and software components, and management overhead costs. As the ISS matures, these costs increase. Increases in the number of agency participants or accessed data sources and in the number of users translate directly into a need for more hardware and software components to maintain acceptable service levels (e.g., response times, throughput). Technology refreshment every five years, at a minimum, is desired (although rarely affordable) to keep the systems maintainable and up-to-date with currently available technologies. Consequently, some Governance Boards have established a fee structure for accessing the ISS. Most fee structures are a sliding scale based on the number of sworn staff in an agency (as opposed to population in an agency's jurisdiction). Larger agencies pay more; the smallest agencies pay the least. Even so, some smaller agencies have difficulty paying a fee, and some agencies have budgets that can change from year to year in an unpredictable manner. Therefore, some ISSs have implemented alternatives for agencies that cannot pay a fee. Agencies can provide a staff member to work for the ISS in lieu of the fee or some other service or hardware/software component. Most ISSs rely on grant funding for developing new capabilities or for enhancements.

Hidden Agency Costs

The costs associated with establishing ISS access to an agency data source can be substantial. Participating agencies need to allocate internal IT staff, when they exist, to support technical staff working for the ISS to facilitate ISS access to their data. This is primarily a one-time event, but it can take significant effort over the course of weeks to accomplish. Secure communications have to be established between the agency data source and the ISS and for users of the agency to access the ISS. For those ISSs that employ a common data schema and code set, data elements in an agency RMS must be mapped (translated) to that common data schema, then extracted, and then the codes must be converted to the common ISS set. The data to be shared is then loaded into a repository located at the agency (distributed model) or into a centralized repository. These ETL costs can be substantial, particularly if the agency RMS is an old system. Once the initial data load is completed, a capability is needed to automatically update the data every 24 hours at a minimum (more frequent updating is desirable). Participating agencies need to allocate staff to oversee the daily uploads and the status of communication links. Occasionally, upload processes can terminate and the data available in the ISS becomes out of sync with the data in the RMS. Warrant data, in particular, can quickly become unreliable. In addition, agency staff need to be trained to make corrections to the data when necessary.

Participating agencies need to allocate staff to manage user names, passwords, and access privileges. For a large agency, this can be a significant effort.

Further, participating agencies are responsible for the actions of their users (and guest users); consequently, they need to allocate staff to perform periodic audits of ISS usage by their staff. These audits commonly identify anyone who is using the system in a manner that indicates they need more training as opposed to identifying a person who is misusing the system.

The most significant cost to agencies may be associated with dedicated training programs. Removing an officer from the field to attend a dedicated training session can be too costly for some agencies.

Finally, the IT staff of the participating agency must maintain the devices used by agency staff to access the ISS. In some cases, this can also be very costly. For example, if a certain version of browser software is needed, older devices may need to be updated. It is also critical for agencies accessing the ISS to have current virus protection software installed and updated regularly on all devices with connectivity to the ISS; the interviewed ISSs recommended that virus protection for all end-users should be kept up-to-date.

6.1.5 Participating Agency Responsibilities

It should not be overlooked that agencies participating in an ISS share responsibility for the success of the ISS, especially in the quality of information shared. Individual agencies are responsible for granting their staff access to the ISS and to the specific functions and data sources that each person is authorized to access. Each agency is responsible for the data it makes available to the ISS, including maintaining the accuracy and currency of the data. Each agency decides what data it will make available. Not every agency provides the same data. One agency may not collect a type of data, another may not share certain data outside of their agency (such as narrative data). Some ISSs allow guest users—users from other agencies. Guest users are the responsibility of the member agency that grants access to those users. Typically, access is granted by the Governance Board to users from non-participating agencies, such as federal and state agency law enforcement personnel who need to access the ISS. Similarly, users from non-law enforcement agencies may be granted access to a limited subset of functions and data. A background check is performed for all users who access law enforcement information.

6.2 Technical Considerations

In addition to programmatic considerations, there are number of technical considerations that should be addressed by the ISS program. These are primarily associated with decisions regarding the type of architecture to employ, key system capabilities, origin of accessible data, and software rights.

6.2.1 ISS Architecture

One important result from CRISP is that there is not one architecture model that supports all situations or needs. Centralized architectures provide the opportunity to perform analysis on consolidated data, and allow advanced mapping capabilities to be offered. The distributed model allows data to remain under management of the source agency and avoid issues with data duplication such as currency. Mature ISSs seem to evolve towards a hybrid of these. Typically, regardless of the architecture, data that an agency makes available to an ISS is extracted from their internal RMS. The decoupling of the RMS from the ISS has numerous advantages. The RMS is a critical system; any increases in workload to support the ISS could affect the daily operational activities of the agency, in addition to the data security issues external user access may impose.

The architecture and components selected for an ISS have an impact on the cost of establishing and operating the ISS. There are other tradeoffs between desired service levels (e.g., response time, downtime/availability) and cost. Similarly, the number of data sources, the number of data types accessible, the desired functionality of the system, the number of users to support, the different types of devices—such as PDAs, desktops, and MDTs—that can be used to access the system all have an impact on the cost of the system. This is one of the reasons that Sections 4 and 5 distinguish between requirements that must be in an ISS (fundamental) and those that should be in the system but could be added later (optional). Replacement, maintenance, operational, and enhancement costs are all considerations when evaluating a technical approach. The need for backup and recovery capabilities must be factored in as well.

6.2.2 Key System Capabilities

One key capability of any ISS should be information\ de-confliction and the ability to build associations. The ability for the system to help de-conflict multiple entries about the same person, location, or thing is generally the most desired capability. The ability for the system to report known associates—such as persons in a car as documented in an incident report—is also critical. In addition, some systems attempt to identify associates that are not documented in records with unique algorithms that use a combination of data elements and other data sources (e.g., public record data).

Another consideration is ease of use, especially system navigation, which can significantly impact the efficiency in which users can search for information in the ISS. Many successful ISSs have features that let users select information and easily move it (e.g., drag-and-drop) to another query, a mapping capability, an external analysis or charting application, and so forth. Another popular feature in developing leads is the ability to navigate back to previously entered search criteria. The user enters the criteria, gets results, modifies the search criteria, get results, and repeats that process over and over. When the path taken is not leading anywhere, the user can simply navigate back to one of the previous sets of criteria that was more promising. This time the user modifies different search parameters, thereby taking another path to develop leads. Minimizing key strokes and reentry of information is essential.

Another key capability is geo-coding of addresses. In order to support mapping, addresses from the data sources need to be converted to a standardized geo-coding. This conversion process is iterative; some addresses will not convert and need to be corrected. This process can be time-consuming—and therefore expensive.

6.2.3 Non-Law Enforcement Data Sources

In addition to law enforcement information, many ISSs commonly use public record data to develop telephone, address, and associate leads. Numerous state data sources are also used such as employment commission data and DMV. DMV data is highly desired to obtain current photos for identifying a individual. The common background allows the photos to be used for including the individual in a photo lineup. The manner in which this information is used and merged with sensitive law enforcement data may require review by privacy experts. Some ISSs are excluding such data to avoid any issues with privacy advocates; others work with privacy experts to use the information in a manner consistent with privacy laws. This consideration can affect how data is displayed and printed by the system, and how users are authorized to use the data.

6.2.4 Software Ownership

When ISS management contracts for software to be developed, ownership of the software should be negotiated so the ISS is not tied to a specific vendor for future enhancements. While the application may include licensed products (e.g., database software such as Oracle, MS SQL Server), the application software that sits on top of licensed products should be owned by the agency or ISS program that paid for its development. If software rights are not obtained, then the agency or ISS may be dependent on the vendor for future enhancements or modifications.

6.2.5 Vendor and Technology Changes

ISSs are complex integrations of numerous components. Each of these hardware and software components should be “real” products from reputable vendors that are operational in similar environments. All interviewed ISSs reported that products—as well as relationships with vendors—evolve over time. If a vendor is purchased by another company, product support and cost impacts may be experienced. Sometimes, a product is discontinued and will not be maintained after a certain date. The likelihood of such changes is high, and agencies and ISSs need to have contingencies in place to deal with these changes.

7 ISS Program Evaluation: Evaluation Factors and Metrics

Metrics are a set of measures that may be used to assess the success or failure of a system or program.

- A system is a tool—in this case, the software and hardware associated with an ISS and the additional support (system administrators)—needed to operate the components. In assessing systems, metrics are frequently used to track measurable performance quantities, including system response time, reliability, and use.
- A program includes the system, users, policies for applying the system, and operations to which the system is applied. In assessing a program, metrics may be used to track measurable quantities related to operations, such as time, labor, and cost savings realized from implementing a new program.

Difficulties arise when trying to use metrics to assess system or program features that produce qualitative results, presenting the challenge of measuring results that may not be quantifiable. Difficulties also arise when trying to measure results that may be attributed, in part, to factors external to the system or program being evaluated. Yet another difficulty is that the ISS may be one of many system or program resources used that have an impact on operations, which means its role may not be measurable or directly attributed to a case closure, for example. Furthermore, lapses in time between specific use of the system and the noticeable impact on operations may make it difficult to attribute ISS use to specific operations. These difficulties do not prohibit the use of metrics, but care must be taken when defining appropriate metrics and determining appropriate measures to capture the metrics.

As mentioned in Section 1, a metrics methodology for evaluating regional law enforcement ISS and its impact on law enforcement operations was developed as one component of CRISP. A summary of the resulting *Metrics Evaluation for Law Enforcement Information-Sharing Systems* document is provided below.

7.1 Metrics Methodology Background

The CRISP *Metrics Evaluation for Law Enforcement Information-Sharing Systems* document focuses on metrics collection and analysis efforts to evaluate an ISS program in three critical areas as they pertain to agency personnel and public safety:

- **Impact on mission**—evaluated by examining who uses the ISS and how they use it. Potential users include agency personnel from local, regional, tribal, national, and international jurisdictions. The results of the evaluation may be used to enhance the program or to support a decision to continue or discontinue the program.
- **Impact on collaboration**—evaluated by examining whether the ISS program provides the user population what it wants and needs, thus promoting more effective teamwork both internally and across the region. The results of the evaluation may be used to further encourage user-population interest in using an ISS or to facilitate more effective information exchange via the ISS.
- **Quality of the investment in the ISS program**—evaluated by examining the purpose, efficiency, return on investment, and cost-versus-benefit of the ISS program. The results of an evaluation may be used to develop new programs, enhance existing programs, or allocate resources in support of information exchange.

The metrics portion of CRISP included multiple efforts. First, research was conducted on the state of metrics collection in law enforcement with an emphasis on metrics related to ISS programs. This research provided some insight into lessons learned on the use of metrics and identified basic elements needed for an ISS metrics program. Next, metrics evaluation lessons learned were gleaned from the six information-sharing programs listed in Section 1 (CRIMES, InSite, FACTS, CLEAR, FINDER, and ARJIS). These two efforts resulted in development of a detailed, automated approach for developing a metrics collection and analysis program. Afterward, issues and impacts associated with the devised approach were examined to guide its appropriate application.

7.1.1 Summary of the Metrics Methodology

Developing an approach for an ISS metrics collection and analysis program that addresses quantitative and qualitative measures is complex. Therefore, a step-by-step methodology was developed in this study. The methodology includes determining which metrics to collect, how to collect the corresponding data for those metrics, and how to analyze the results. One key requirement of the methodology is that any metrics collection program should place little or no burden on ISS users. Thus, the emphasis is on automated metrics collection, which requires no direct user input, supplemented by infrequent and minimal direct user input.

Determining the issues and impacts associated with an ISS metrics collection program is critical for mitigating circumstances that may hinder the value and reliability of the metrics program. ISS management preparations prior to program implementation are suggested, including the possible addition of staff resources to implement and monitor the program, as well as to analyze the metrics data. A plan for implementing a metrics collection and analysis program is described in *Metrics Evaluation for Law Enforcement Information-Sharing Systems.* The plan, based upon a mapping between ISS objectives and potential metrics, includes the following six steps:

- **Step 1: Define ISS program objectives.** The first step in establishing a metrics collection program is to determine the objectives of the ISS program; these objectives directly impact the types of metrics that need to be collected and the collection process.
- **Step 2: Determine which types of metrics to collect.** There are two primary categories of metrics that are appropriate—metrics for assessing ISS performance and metrics for assessing impact of the ISS on day-to-day operations.
- **Step 3: Determine feasibility of the metrics.** Metrics feasibility is determined by whether or not a metric is collectable and whether or not the metric reflects the objective being assessed in a meaningful and reliable fashion.
- **Step 4: Map ISS program objectives and metrics.** The purpose of mapping metrics to ISS program objectives is to ensure that the proper metrics are being collected and can support the stated objectives.
- **Step 5: Collect metrics.** Developing a metrics collection methodology requires consideration of fundamental statistical procedures, including collection frequency, from whom or what metrics will be collected, a basis for comparison, and verification of collected metrics.
- **Step 6: Analyze metrics collected.** Statistical techniques should be applied to determine variability and relationships between factors affecting the values of the metrics. Statistical techniques will also need to be applied to manage the data and to determine which of the many independent variables should be used to predict values of the dependent variables.

7.1.2 Potential Impacts of a Metrics Program

Metrics collection is a major and challenging operation. Some considerations regarding implementing a metrics program and its impact on policies and resources are listed below, followed by additional technology that may enhance the operation of an ISS metrics collection program.

7.1.2.1 Impact on Policy and Resources

Functional requirements will need to be formally developed to ensure that appropriate metrics can be collected. Many of the proposed metrics are not readily available, and supporting data is not typically collected for law enforcement operations. In addition, the techniques for automatic electronic capture of many of the metrics must be specified. Many of these requirements will be applicable to various ISSs and should be shared among those ISSs. Significant work will need to be done to define functional capabilities and develop supporting software in order to realize the functional requirements. These functional capabilities should define the specific transactions that must be tagged and tracked, the algorithms needed to generate metric values based upon these transactions, and the algorithms needed to analyze the metrics. Coordination between users, system planners, and software developers will be critical. While functional requirements also impact technology, recognizing the need and the decision to incorporate the requirements for metrics collection must be addressed first during ISS policy and planning.

The decision to make participation in the ISS voluntary or mandatory will need to be made and will affect ISS policy. An ISS will not be used more than minimally required unless it is beneficial to the users. Therefore, voluntary-versus-mandatory participation in the ISS may affect the quality of the metrics. For example, high usage and participation rates may be very meaningful if use is voluntary but may be meaningless if use is mandatory. An ISS with voluntary participation that has low usage rates may provide a strong indication that the ISS is not viewed as useful, whereas voluntary participation and high usage rates may indicate that the ISS is viewed as useful. Significantly higher than expected usage and participation rates for a mandatory ISS may be meaningful, as this may be an indication that the ISS is useful. Mandating usage may also encourage otherwise reluctant users to try the system and learn how to use it effectively.

Development or selection of a comparison group should be completed before the ISS is implemented. Planning for the comparison group should be part of the planning for the metrics collection program. The law enforcement environment is very dynamic. Therefore, it is not possible to hold external ISS factors constant when attempting to determine whether the ISS contributes to meeting its objectives. The use of a comparison group attempts to account for the impact of some of these external factors. Metrics must be interpreted very carefully and supplemented by success stories from the user population in order to determine whether the ISS is useful.

Additional resources will most likely be needed if a metrics collection program is implemented. Software developers will be needed to program the functional capabilities necessary to tag transactions in order to collect the metrics. Technical support will be needed to ensure proper collection of metrics and to monitor the collection process. Statistical analysts will be needed to define the metrics, to map metrics to objectives, and to compile, analyze, and interpret the metrics. Additional analysts may be needed to help sort through the increased information that users will obtain with an ISS and to determine the relevance of the information found via the ISS. ISS advocates have proved beneficial to the FACTS and FINDER programs by maintaining communication with the users on how the systems are being used, collecting success stories, and passing along recommended improvements. The costs associated with the additional resources, as well as cost of the metrics collection program, should be included when planning for the ISS.

There are several other considerations regarding the overall ISS program that may affect the metrics collection process. ISS management and governance have a significant influence on how users view the ISS. In addition, total cost of ownership should be determined—and planned for—early in the ISS planning process so that the program is sustainable even after initial funding has been exhausted. These two factors will affect operation of the ISS program, operation of the metrics collection program, and ultimately, a user's ability to effectively use the system and his/her desire to provide meaningful input on system use.

7.1.2.2 Impact on Technology

It may be beneficial to have a secure database for ISS programs willing to share their metrics collection methodology and functional requirements, metrics data, and conclusions regarding the extent to which ISS objectives are being met. This information would provide guidance to agencies considering an ISS or considering a metrics collection program. The information would also serve as a source of comparison data for ISS programs. Interested programs would need to coordinate this effort and set policies for its use.

It may also prove beneficial to use a decision tool to guide ISS planners through the process of developing a metrics collection program. The tool would have two roles: help planners define a metrics collection program and then analyze and interpret the metrics collected. The tool could guide program definition by soliciting ISS objectives from the planner, followed by generating a map between the objectives and feasible metrics. The planner could then input baselines, target levels, or other comparison values for each metric. The metric values would then be extracted from the ISS and analyzed statistically by the tool, with results presented in a summary report.

7.1.3 Recommendations for Metrics Collection and Analysis

Key recommendations for a metrics collection and analysis program are presented below:

- There must be a formal plan in place for metrics collection so that useful and appropriate metrics are collected and users are not burdened with the collection process.
- A preliminary behavioral study on how best to obtain quality input from users would be beneficial.
- The significant value of qualitative information as metric data should be recognized.
- A combination of metrics should be used to assess each objective rather than considering each metric as distinct from the rest.
- The relationship between law enforcement agencies and the broader criminal justice system can be leveraged.
- It is important to acknowledge that some metrics will provide an indication of the usefulness of the ISS, but they may not provide definitive relationships between ISS use and meeting of ISS objectives.
- Planning for and implementing a metrics collection program is a long-term process, but taking some actions early on may facilitate the effort.
- ISS metrics may also be used as a design tool to plan for, evaluate, or improve other law enforcement programs.
- It may be helpful to expand this research and more closely examine ISS and non-ISS programs outside of the criminal justice system that rely on measures of effectiveness and seek to produce primarily qualitative results.

7.2 Requirements to Support Metrics Methodology

As stated in Section 7.1.1, there are two primary categories of metrics that are appropriate: metrics for assessing ISS performance and metrics for assessing impact of the ISS on day-to-day operations.

Metrics for assessing ISS performance are typically quantitative and reflect existing system operations, functionality, and capabilities. When evaluating system performance metrics, it is important to take into consideration that ISS host-system performance may be impaired by individual agency system performance. System features and characteristics that are critical for meeting ISS objectives are used to categorize the various metrics. There are four main metric categories for assessing system performance:

- Access to ISS services
- Capacity of the ISS
- Search and retrieval
- Information security

Metrics for assessing the impact of the ISS on day-to-day operations are typically qualitative and may help evaluate how the ISS is being used. These metrics are needed to assess the effectiveness of the ISS and to determine in what ways the ISS helps to prevent and solve crime. Some of these qualitative measures may be converted to quantitative metrics. Development of the bulleted list below began with abstract types of observations that should be measured and continued on to more quantitative, concrete measures representing the abstract observations. A combination of metrics may be needed to measure one abstract observation. System and program features and characteristics that are critical to meeting ISS objectives are used to categorize the various metrics. The main metric categories for assessing impact on day-to-day operations are listed below:

- Link association
- Data quality

- Performance (occurrences)
- Performance (time savings)
- Efficiency
- Participation
- Productivity
- Usefulness
- User satisfaction
- Utilization

All of the main metrics categories listed above are taken from the *Metrics Evaluation for Law Enforcement Information-Sharing Systems* document.

Many of the requirements defined in this handbook propose the use of ISS transactions to capture metrics. Additional metrics may be captured by surveys or ISS program information from agencies regarding ISS use. Due to the complexity of metrics collection, additional work is required to actually define how to determine the value of many metrics. Therefore, determining the requirements needed to capture such metrics is ongoing, and all related requirements may not be reflected in this handbook. The overarching requirements needed for the collection, compilation, and analyses of metrics are found throughout this handbook and are identified below. The parent section is included for completeness, followed by the specific sections containing the requirements. Note that these requirements allow for any metrics—as determined by ISS governance/management and participating agencies—to be included in an ISS program evaluation:

- **Section 4.1.2—Common Data Management Requirements.** Sections 4.1.2.6 through 4.1.2.10 allow for the entry of user feedback into the ISS. User feedback should consist of success stories, comments, and survey responses. User feedback should be used to help assess the value of the ISS and its various features.
- **Section 4.2.1—Query.** Sections 4.2.1.28 through 4.2.1.32 allow for the query and viewing of user feedback contained in the ISS.
- **Section 4.2.3—System Administration.** Section 4.2.3.15 through 4.2.3.35 allow for audit logs. Audit log contents and features are included, as well as capabilities to manipulate, search, and capture audit log data. Audit log report generation is also reflected. Audit log information is a critical component of metrics collection because it provides basic data on time references, types of transactions, operating statistics, and system access.
- **Section 5.3.1—Metrics Collection.** All of Section 5.3.1 is directly relevant to metrics, and it allows for the capture, entry, retrieval, and compilation of all types of metrics data. Metrics analysis and report generation are also reflected.

7.2.1 Relationship between Metrics and Requirements

The reader is referred to the Metrics Evaluation for Law Enforcement Information-Sharing Systems document for an extensive set of metrics associated with each of the metrics categories listed above. Table 7-1 provides brief descriptions of the metric categories and a mapping of the metric categories to the requirements and guidance from Sections 4, 5, and 6 of this handbook. The requirements and guidance identified in Table 7-1 are those that most directly support the capture and computation of the specific metrics associated with the metric categories.

The requirements and guidance identified in Table 7-1 are in addition to the overarching requirements provided above. Some of the specific metrics may be captured by a single requirement, while most metrics need multiple requirements for their values to be captured and calculated. A given set of requirements may be manipulated in various ways to generate multiple metrics. In general, measures may be captured or derived from any of the following: ISS transaction data, compilation of transaction data, individual users, agency users, ISS governance/management, and system administrators. Algorithms will need to be developed to compile the various metrics. This handbook contains both fundamental and optional requirements. Individuals responsible for developing final requirements for an ISS must ensure that the selected requirements fully support the collection, compilation, and analyses of metrics that ISS governance/management and participating agencies choose to include as part of an ISS program evaluation.

Table 7-1 Functional and Operational Requirements Supporting Metrics Methodology

Metric Category	Metric Category Description	Section Reference
Access to services	Response times; reliability of access to ISS and data by authorized users	4.2.3, 5.3.1, 5.3.2, 5.3.3, 5.4.1
Capacity of the ISS	Number of users allowed due to technology constraints	4.2.3, 5.3.1, 5.3.2, 5.3.4, 6.1.2 (agencies and governance must monitor)
Search and retrieval	Tools available in the ISS; links to other databases or systems	4.1.1, 4.1.2, 4.2.1, 5.3.1
Information security	Extent to which security is successful; security reliability	4.2.2, 5.1, 4.2.3, 5.2., 5.3.1, 5.3.4
Link association	Extent to which users access information from other agencies, jurisdictions	4.2.2, 4.2.3, 5.3.1
Data quality	Detail, completeness, accuracy, locate-ability of data available via the ISS; quality of reports	4.1.1, 4.1.2, 4.2.1, 4.2.2, 5.3.1, 6 (agencies and governance must monitor)
Performance (occurrences)	Frequency with which ISS information assisted with various law enforcement operations	4.1.2, 4.2.1, 4.2.3, 5.3.1
Performance (time savings)	Time to complete law enforcement operations	4.1.2, 4.2.1, 4.2.3, 5.3.1
Efficiency	Costs of ISS relative to ISS impact on crime statistics	4.2.3, 5.3.1, Section 6 (agencies and governance must monitor)
Participation	Number of eligible ISS users; extent to which eligible records/reports are submitted by eligible ISS users; and interest among users not participating in the ISS	4.2.3, 5.3.1, Section 6 (agencies and governance must monitor)
Productivity	Amount of effort required by users to generate successes; allocation of resource time; tips from community	4.1.2, 4.2.1, 4.2.3, 5.3.1, 6.1.2
Usefulness	How the ISS is used to assist law enforcement operations; value of ISS information	4.1.2, 4.2.1, 4.2.3, 5.3.1
User satisfaction	Ease of use and satisfactions with training	4.1.2, 4.2.1, 5.3.1, 5.4.4, 6.2.2
Utilization	Extent to which the ISS is accessed and queried by users; consider mandatory and voluntary use	4.2.3, 5.3.1, Section 6 (agencies and governance must monitor)

Appendix A
Glossary of Terms and List of Acronyms

A.1 Glossary of Terms

Adequate Survivability	The ability of the ISS to continue to function at an acceptable level of performance during and after a natural or man-made disturbance.
Agency	Refers to a law enforcement entity that is required to sign an agreement to become a member of the ISS.
Assignments	Types of operations that are allocated to a user or a group of users.
Associates/Associations	People/people, locations.
Attributes	The characteristics associated with a person, place or thing.
Authorized Agency	A member agency of the ISS that is authorized to provide information to be shared by other member agencies. Authorized agencies designate which of their personnel can become authorized users of the ISS.
Authorized User	The end user who is authorized to log onto the system and access information through the system's functionality.
Availability	Is calculated as follows: $\text{Availability} = \dfrac{\text{System Uptime}}{\text{System Uptime + System Downtime}}$
CompStat	The regularly scheduled briefings that are conducted by law enforcement agencies using computerized statistics of crime in their immediate jurisdictions and in surrounding jurisdictions.
Data	Information that is collected, stored, retrieved, and disseminated within and among systems.
Data Element	A compendium of information related to a specific type of data that is to be collected, stored, retrieved and disseminated in a system.
Data Repository	The physical container or database that is the host for the data in a system.
De-confliction/de-conflict	The software function for eliminating contradictory data returned in query responses.
Electronic Photographic Lineup	The software function for displaying a sequence of Individuals' photographs representing similar personal attributes for visual comparison purposes.
Fundamental	Necessary for basic effectiveness.
Geo-coded	Coding of location by latitude and longitude.

GIS Map

Geographical information systems maps; uses geo-coded Methodology.

Google™-like Text Search

The proprietary text search capability for retrieving information from the system (e.g., WWW) that matches text strings entered by the user

Governance Board

The persons (or committees or member agencies) that make up a body for the purpose of administering the ISS by establishing the policies and procedures and securing funding for the ISS

Information Exchange/ Exchange Information

Giving **and** receiving of information; may or may not involve a structured electronic system (e.g. exchange may occur via phone, fax, e-mail, verbal communication, driving to pick-up/deliver information from another agency/jurisdiction, meetings, task force, working groups)

Information-Sharing/ Share Information

Giving **and/or** receiving of information; may or may not involve a structured electronic system (e.g. sharing may occur via phone, fax, e-mail, verbal communication, driving to pick-up/deliver information from another agency/jurisdiction, meetings, task force, working groups)

ISS

A collection of software and hardware components used to perform information-sharing functions; additional support (system administrators) needed to operate the components are also included as part of the information-sharing system

ISS Program

Effort encompassing the information-sharing system, users, policies for applying the system, and operations to which the system is applied

Lexicon

A lexicon is a repository of words and knowledge about those words. As applied to information-sharing, the lexicon is a compilation of terms, each with a prescribed meaning that is pertinent to the collection, storage or sharing of information

Link Analysis

The software function for linking seemingly unrelated data elements together based on person, place or thing attributes

Management Board

The persons (or committees) who make up a body for the purpose of operating the ISS by carrying out the established policies and procedures of the ISS

Mapping

The software function for visually displaying a geographical representation of physical locations or events that occur at those locations

Name

Any name a person uses – exact name, alias, phonetic spelling of name

Non-availability

Due to individual client hardware or operating system problems will not be counted as System Downtime. Downtime due power outages or other problems beyond the control of the system contractor that affect system operations will not be counted as either System Uptime or System Downtime.

Officer Notification

The software function for communicating to a law enforcement officer a pending noteworthy event such as a BOLO.

Optional

Not absolutely necessary, but adds value.

Phonetic Text Search

A query that is run to extract the data that matches the phonetic value of the search criteria. The phonetic value is the spelling of the text as it relates to how the text sounds or is spoken.

Police Officer

Sworn law enforcement officer including patrol/field officer, detective (investigator), crime analyst, intelligence analyst, and command staff.

Practitioner

One who practices law enforcement operations; an end user of a law enforcement system.

Public User

A member of the general public who accesses a system to provide and receive information.

Query by User

Process of issuing a request **and** receiving a response.

Query by System

Process of issuing a request **and** retrieving a response.

Recorded Attribute

A named value or relationship that has been stored for a data element.

RMS

Electronic records management system; not including public records system.

Record

Information or data on a particular subject collected and preserved.

Region

Area consisting of agencies with which one may coordinate activities; may extend over city, county, state boundaries; multi-jurisdictional area.

Regional Law Enforcement Information-Sharing System

Electronic system containing information, originating from local law enforcement agency records management systems, that is shared among law enforcement agencies within a region; participation by an agency in a regional law enforcement information-sharing system allows individuals within the participating agency to query and/or contribute information from desktop or laptop computers (and other such equipment); participation may be formalized by an agreement with regional law enforcement information-sharing system management or governance.

Reliability

The ability of a system to perform a required function under stated conditions for a specified period of time.

Save

The software feature that enables data elements, user queries, and reports to be saved for subsequent access by the user.

Single Sign-on

The act of signing on once (providing a UserID and Password) thereby achieving access to multiple systems or e-services without having to re-establish the identity of the person signing on.

Survivability

The quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance.

Systems of Record

The official group of records of a system that is under the control of the recognized system owner and from which information may be retrieved by the name of the individual, or by some identifying number, symbol, or other personal identifier.

System Downtime

Cumulative clock period when the system is not available. System Downtime will include periods during which the system is unavailable due to operations being switched from a primary to a backup server.

System Uptime

Cumulative clock periods when the system is available to the users. System Uptime will not be counted unless the system has been available for a period of 5 consecutive minutes.

User

Nominally, this refers to the end user of a system, i.e. the person for which the system was implemented to support. In this document, an end user is assumed to be an authorized law enforcement user. In some instances, depending on who is performing the action, the term user may refer to agency and is assumed to be an authorized ISS member agency.

User Feedback

Success stories; comments or suggestions on the ISS; surveys made available via the ISS .

Wildcard Search

Search for data without having to supply the complete spelling of the subject being searched.

Work-in-Progress

The suspended user query request process consisting of stored query parameters and partial query results.

A.2 List of Acronyms

ARJIS	Automated Regional Justice Information System
BOLO	Be On The Lookout
CAD	Computer-Aided Dispatch
CBT	Computer-based training
CCJT	Center for Criminal Justice Technology
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordinating Council
CLEAR	Citizen and Law Enforcement Analysis and Reporting (System)
CompStat	Computerized Statistics
CONOPS	Concept of Operations
COOP	Continuity of operations
CRIMES	Comprehensive Regional Information Management Exchange System
CRISP	Comprehensive Regional Information-Sharing Project
DBMS	Database management system
DE	Development Environment
DMV	Department of Motor Vehicles
ETL	Extract, Transfer, and Load
FACTS	Factual Analysis Criminal Threat Solution (System)
FBI	Federal Bureau of Investigation
FINDER	Florida Information Network for Data Exchange and Retrieval (System)
GJXML	Global Justice Extensible Markup Language

Global JXDM	Global Justice Extensible Markup Language Data Model (also GJXDM)
Global JXDD	Global Justice Extensible Markup Language Data Dictionary (also GJXDD)
GUI	Graphical user interface
InSite	Intelligence Site (System)
ICD	Interface Control Document
ISS	Information-sharing system
LEITSC	Law Enforcement Information Technology Standards Council
LEO	Law Enforcement Online
MDT	Mobile data terminal
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCISP	National Criminal Intelligence Sharing Plan
NIEM	National Information Exchange Model
NIJ	National Institute of Justice
ODBC	Open database connectivity
OJP	Office of Justice Programs
PDA	Personal Data Assistant
PE	Production Environment
PERF	Police Executive Research Forum
RFI	Request for Information
RFP	Request for Proposal
RISS	Regional Information-Sharing Systems®
RMS	Records Management System
SBU	Sensitive But Unclassified
SLA	Service Level Agreement
SQL	Structured query language
SSL	Secure Sockets Layer
TE	Test Environment
WWW	World Wide Web
XML	eXtensible Markup Language

This page intentionally left blank

Appendix B
ISS Capabilities/Requirements and NCISP Recommendations

In February 2005, the Department of Justice, Office of Justice Programs (OJP) sponsored a revision of the National Criminal Intelligence Sharing Plan (NCISP). The Plan provides 28 explicit recommendations in an effort to develop "solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence."[5] These recommendations were referenced and considered when developing this handbook. In particular, 11 of the recommendations presented in the NCISP February 2005 revision lend themselves to law enforcement information-sharing systems (ISSs) as they relate to this handbook and the other CRISP documents. The 11 recommendations cited are listed below (as they are presented in the NCISP February 2005 revision, pages v-viii).

Recommendation 7: Local, state, tribal, and federal law enforcement agencies must recognize and partner with the public and private sectors in order to detect and prevent attacks to the nation's critical infrastructures. Steps should be taken to establish regular communications and methods of information exchange.

Recommendation 18: Training should be provided to all levels of law enforcement personnel involved in the criminal intelligence process. The training standards, as contained within the National Criminal Intelligence Sharing Plan, shall be considered the minimum training standards for all affected personnel. Additionally, recipients of criminal intelligence training, as recommended in the National Criminal Intelligence Sharing Plan, should be recognized and awarded certificates for successful completion of training.

Recommendation 20: In order to support agency tactical, operational, and strategic needs, law enforcement agencies are encouraged to consider an automated, incident-based criminal records tracking capability, in addition to traditional case management and intelligence systems, to use as an additional source for records management and statistical data. These systems should be Web-based and configured to meet the internal reporting and record-keeping needs of the component, in order to facilitate the exportation of desired data elements—without the need for duplicate data entry or reporting—to relevant statewide federal criminal information programs.

Recommendation 21: The Regional Information-Sharing Systems® (RISS) and the Federal Bureau of Investigation (FBI) Law Enforcement Online (LEO) systems, which interconnected September 1, 2002, as a virtual single system, shall provide the initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability. This nationwide sensitive but unclassified communications backbone shall support fully functional, bidirectional information-sharing capabilities that maximize the reuse of existing local, state, tribal, regional, and federal infrastructure investments. Further configuration of the nationwide sensitive but unclassified communications capability will continue to evolve in conjunction with industry and the development of additional standards, and the connection of other existing sensitive but unclassified networks.

Recommendation 22: Interoperability with existing systems at the local, state, tribal, regional, and federal levels with the RISS/LEO communications capability should proceed immediately, in order to leverage information-sharing systems and expand intelligence sharing.

Recommendation 23: The Criminal Intelligence Coordinating Council (CICC) shall work with Global's Systems Security Compatibility Task Force to identify and specify an architectural approach and transitional steps that allow for the use of existing infrastructures (technology, governance structures, and trust relationships) at the local, state, tribal, regional, and federal levels, to leverage the national sensitive but unclassified communications capabilities for information-sharing. This strategic architectural approach shall ensure interoperability among local, state, tribal, regional, and federal intelligence information systems and repositories.

[5] Appendix C, Reference 10

Recommendation 24: All agencies, organizations, and programs with a vested interest in sharing criminal intelligence should actively recruit agencies with local, state, tribal, regional, and federal law enforcement and intelligence systems to connect to the nationwide sensitive but unclassified communications capability. Such agencies, organizations, and programs are encouraged to leverage the nationwide sensitive but unclassified communications capability, thereby expanding collaboration and information-sharing opportunities across existing enterprises and leveraging existing users. Moreover, participant standards and user vetting procedures must be compatible with those of the currently connected sensitive but unclassified systems, so as to be trusted connections to the nationwide sensitive but unclassified communications capability.

Recommendation 25: Agencies participating in the *National Criminal Intelligence Sharing Plan* are encouraged to use *Applying Security Practices to Justice Information-Sharing* as a reference document regarding information system security practices. The document was developed by the Global Security Working Group to be used by justice executives and managers as a resource to secure their justice information systems and as a resource of ideas and best practices to consider when building their agency's information infrastructure and before sharing information with other agencies.

Recommendation 26: Agencies are encouraged to utilize the latest version of the Global Justice eXtensible Markup Language (XML) Data Model (Global) and its component Global Justice XML Data Dictionary (Global JXDD)7 when connecting databases and other resources to communication networks. The Global JXDM and Global JXDD were developed to enable interoperability through the exchange of data across a broad range of disparate information systems.

Recommendation 27: In order to enhance trust and "raise the bar" on the background investigations currently performed, law enforcement agencies must conduct fingerprint-based background checks on individuals, both sworn or nonsworn, prior to allowing law enforcement access to the sensitive but unclassified communications capability. Background requirements for access to the nationwide sensitive but unclassified communications capability by law enforcement personnel shall be consistent with requirements applied to the designation and employment of sworn personnel, as set by the participating state or tribal government, so long as, at a minimum, those requirements stipulate that a criminal history check be made through the FBI and the appropriate local, state, and tribal criminal history repositories and be confirmed by an applicant fingerprint card. Additionally, a name-based records check must be performed on law enforcement personnel every three years after the initial fingerprint-based records check is performed.

Recommendation 28: The CICC, in conjunction with the OJP and the connected sensitive but unclassified systems, shall develop an acquisition mechanism or centralized site that will enable law enforcement agencies to access shared data visualization and analytic tools. The CICC shall identify analytical products that are recommended for use by law enforcement agencies in order to maximize resources when performing intelligence functions, as well as a resource list of current users of the products.

Appendix C
References

CRISP Products

1. System Documentation for the Automated Regional Justice Information System (ARJIS), February 2006.
2. System Documentation for the Citizen and Law Enforcement Analysis and Reporting (CLEAR) System, May 2006.
3. System Document for the Comprehensive Regional Information Management Exchange System (CRIMES), January 2006.
4. System Documentation for the Factual Analysis Criminal Threat Solution (FACTS) System, May 2006.
5. System Documentation for the Florida Information Network for Data Exchange and Retrieval (FINDER) System, May 2006.
6. System Documentation for the Intelligence Site (InSite) System, February 2006.
7. Concept of Operations, March 2006.
8. ISS Interactive Mapping Tool
9. Metrics for the Evaluation of Law Enforcement Information-Sharing Systems, March 2006.

Additional References

10. Global Intelligence Working Group, National Criminal Intelligence Sharing Plan, Revised February 2005.
11. The SAFECOM Program, Department of Homeland Security, Statement of Requirements for Public Safety Wireless Communications & Interoperability, Version 1.1, January 26, 2006.
12. The Law Enforcement Information Technology Standards Council, DRAFT Standard Functional Specifications for Law Enforcement Records Management, Systems (RMS), V.1, August 2005.
13. The Law Enforcement Information Technology Standards Council, Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD), Systems, V.1, August 2005.
14. Noblis for Metropolitan Washington Council of Governments, Requirements for the National Capital Region (NCR) Law Enforcement Information-Sharing System (NCR-LEISS), June 30, 2005.
15. Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World, Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal, and Federal Level: Law Enforcement Intelligence Component, Version 1.0, July 2005.
16. National Institute of Standards and Technology, FIPS 140-2, available at URL: *http://csrc.nist.gov/cryptval/140-2.htm*
17. National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook, NIST 800-12, available at URL: *http://csrc.nist.gov/publications/nistpubs*
18. National Institute of Standards and Technology, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST 800-14, available at URL: *http://csrc.nist.gov/publications/nistpubs*
19. National Institute of Standards and Technology, Guide for Developing Security Plans for Federal Information Systems, NIST 800-18, available at URL: *http://csrc.nist.gov/publications/nistpubs*
20. National Criminal Justice Reference Service, PRIVACY AND SECURITY OF CRIMINAL HISTORY INFORMATION - AN ANALYSIS OF PRIVACY ISSUES, available at URL: *http://www.ncjrs.gov/app/publications/Abstract.aspx?id=49544*

This page intentionally left blank