Document Title:	**Comprehensive Regional Information System Project Volume 2: Concept of Operations**
Author(s):	**Noblis**
Document No.:	**219378**
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 2

Concept of Operations

NOBLIS TECHNICAL REPORT
MTR-2006-036
Contract Number 2001-LT-BX-K002

noblis
For the best of reasons

Center for Criminal Justice Technology

MTR-2006-036
Noblis Technical Report

Comprehensive Regional Information-Sharing Project, Volume 2

Concept of Operations

January 2007

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

The Comprehensive Regional Information-Sharing Project (CRISP) Concept of Operations (CONOPS) document binds together the interviews, documentation, and analysis work performed through the partnership between Noblis' Center for Criminal Justice Technology (CCJT) and the National Institute of Justice (NIJ). With the current focus on information-sharing, law enforcement agencies need such a CONOPS to guide them in making informed decisions when establishing regional law enforcement information-sharing systems (ISSs). This document will also help other law enforcement agencies understand the best practices for achieving success and how to overcome the challenges they may face.

This CONOPS document focuses on how information-sharing has evolved from supporting traditional agency needs and roles to supporting those found in an agency participating in an ISS. Agencies learn the challenges encountered in forming an ISS with respect to organizational, legal, and funding constraints. This document compares information-sharing methods with an ISS to information-sharing methods without an ISS. The information-sharing needs and system evolution discussion prepares agencies for setting realistic and targeted goals.

This CONOPS document covers the law enforcement practitioner's best practice approaches for constructing components for an ISS; these approaches range from the ISS program's governance structure to lessons learned about technical system design and implementation. Such guidance helps answer the following difficult questions:

- Which approach best meets the information-sharing needs given the political challenges, financial limitations, and technological resources typically found in law enforcement agencies?
- Have other comparably sized agencies implemented a similar function, program, or technology?
- What issues are associated with picking one information-sharing model approach over another based on actual practitioner experience?

After understanding the background and process of forming an ISS, agencies see the best practices that current, mature ISS organizations have found to achieve success in sharing law enforcement information. Starting with a set of goals and objectives, the surveyed ISS organizations provide example objectives, metrics, and measures of effectiveness. ISS functional best practices are presented in this document in several key areas, such as the type of queries frequently used, type of data shared, and analytical capabilities. The operational system architectures and practices of surveyed ISS organizations are also described.

With assistance from the Police Executive Research Forum (PERF), a national survey was conducted that gathered data on the information-sharing needs of law enforcement agencies around the country. The results of this survey are incorporated into the discussion in this document and support the general findings of CRISP research that are also echoed by the interviewed practitioners.

Most of the surveyed ISS organizations pointed out the issues and impacts of creating an ISS. This document concludes by providing agencies with the operational and organizational considerations that will shape the direction and effectiveness of any new ISS. Agencies also share critical success factors and additional lessons learned. Key trends and common themes are highlighted as important items for agencies to note and factor into their ISS implementation planning.

This page intentionally left blank

Acknowledgements

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 from the following law enforcement ISS organizations:

- 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), based 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

These individuals provided detailed information that was collected as part of the overall CRISP effort and provided the basis for much of the information in this document.

The authors especially thank the following individuals from the organizations above for all 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 members of the Police Executive Research Forum (PERF) who conducted the national survey, and 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 (NCIS), Washington, DC
- 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, Chicago 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 would like to extend special thanks to all of the law enforcement agencies that 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 also wish 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
- Mr. William Ford, Program Manager, National Institute of Justice
- Ms. Michele Moses, Technical Program Analyst (contractor), National Institute of Justice
- Mr. Phil Ramer, Senior Research Associate, for Intergovernmental Research
- The Members of the Global Intelligence Working Group

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Figures

Tables

This page intentionally left blank

How to Use This Document

The Comprehensive Regional Information-Sharing Project (CRISP) Concept of Operations (CONOPS) is a result of research into regional law enforcement information-sharing. The CONOPS provides an overview of best practices, recommendations, and ideas for planning, implementing, and operating a regional law enforcement information-sharing system (ISS).[1] This document is important to anyone who is interested in establishing a regional ISS or planning enhancements to existing regional ISSs. It will guide them toward success by sharing the lessons learned and experiences of those who have implemented and are operating ISSs.

A detailed *System Document* has been prepared for each of six site visits; these documents present the in-depth findings from each site. They also provide a view of how each organization came into existence; the information shared; the approach to governance and management; functional, technical, and operational analyses; specific recommendations; and critical success factors. The companion system documents augment the information contained in this CONOPS and contain more in-depth information on the individual organizations that participated in the CRISP detailed interviews.

Through the analysis of the initial survey data and interview notes, the CONOPS also introduces another document that takes a first look at ISS metrics and evaluation factors. Every organization interested in sharing regional information will need a vetted means to justify their expenditures and to learn what does and does not work and where best to spend scarce resources. The main product of CRISP research is *A Practitioner's Handbook for Regional Law Enforcement Information-Sharing Systems: Preliminary Requirements* document; the Preliminary Requirements document contains the requirements to develop an ISS that satisfies law enforcement information-sharing needs and incorporates the best practices of operational ISSs.

The following terms are used throughout the CRISP documents and are defined here so that their intended meanings will be interpreted consistently in each document.

- **Information exchange/exchange information**—Giving *and* receiving of information
- **Information-sharing/share information**—Giving *and/or* receiving of information
- **Information-Sharing Program**—Effort encompassing the ISS, users, policies for applying the system, and operations to which the system is applied
- **Information-Sharing System**—A collection of software and hardware components used to perform information-sharing functions; additional support (such as system administrators) needed to operate the components are also included as part of the ISS
- **Region**—Area consisting of agencies with which a user 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 law enforcement agency records management systems that is shared among law enforcement agencies within a region
- **System of Record**—The *originating* or *authoritative* system source of data or information; systems that store copies of data or that store data obtained from other data sources (from an agency record management system); are not systems of record

[1] Typical regional law enforcement ISSs contain law enforcement information originating from local agency records management systems; this information is shared with other agencies within a region via a system that individuals within agencies can query from their desktop computer (or other equipment, such as a mobile data terminal or a handheld device).

This page intentionally left blank

1 Introduction

As a result of identified weaknesses in information-sharing practices, the need to share information among local, state, and federal criminal justice agencies is currently a highly visible topic in this country. Law enforcement agencies now need to access regional data to better understand cross-jurisdictional crime. A number of law enforcement and justice agencies have recognized these needs and established information-sharing systems (ISSs). Many state and local law enforcement agencies obligate large portions of their yearly operating budgets to support and develop such multi-jurisdictional ISSs. A number of regionally based systems exist, and more are coming online every year. These systems have been developed independently because organizations recognized that electronic information-sharing could result in significant labor savings gained from time efficiencies. In addition to being able to perform a function faster by accessing data immediately, agencies also realize improvements with data quality because data that was previously captured in hand-written reports is now entered into computers.

While regional efforts exist and continue to come online, there is only limited knowledge and analysis of how these ISSs were developed and currently operate. Local and state agencies are seeking approaches and solutions that fit their specific situation and needs. By studying established ISSs, law enforcement agencies around the nation can benefit from the experience already gained and adopt a strategy that will work for them.

The Comprehensive Regional Information-Sharing Project (CRISP) is beginning to address this need by investigating and documenting the management, functional, and operational characteristics of selected law enforcement ISSs around the country. The project addresses the systems' functional and the technical characteristics, including governance, how the system supports law enforcement functions, and what information is being delivered to law enforcement personnel.

1.1 Background

Following the direction of federal recommendations and guidelines, such as the National Criminal Intelligence Sharing Plan (NCISP), the National Institutes of Justice (NIJ) partnered with Noblis' Center for Criminal Justice Technology (CCJT) to identify and define the policy and programmatic concepts and functional, operational, and technical characteristics associated with sharing law enforcement information regionally. Under the direction of The Global Justice Information-Sharing Initiative (Global),[2] Noblis conducted interviews with several major regional systems during 2005 (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)
- 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 from published sources. Appendix C describes the methodology used in surveying the regional systems. In addition to detailed interviews, during the first half of 2006, a national survey was conducted to identify individual law enforcement regional information-sharing needs.

This Concept of Operations (CONOPS) is based on the results of the research. This research also devel-

[2] 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.

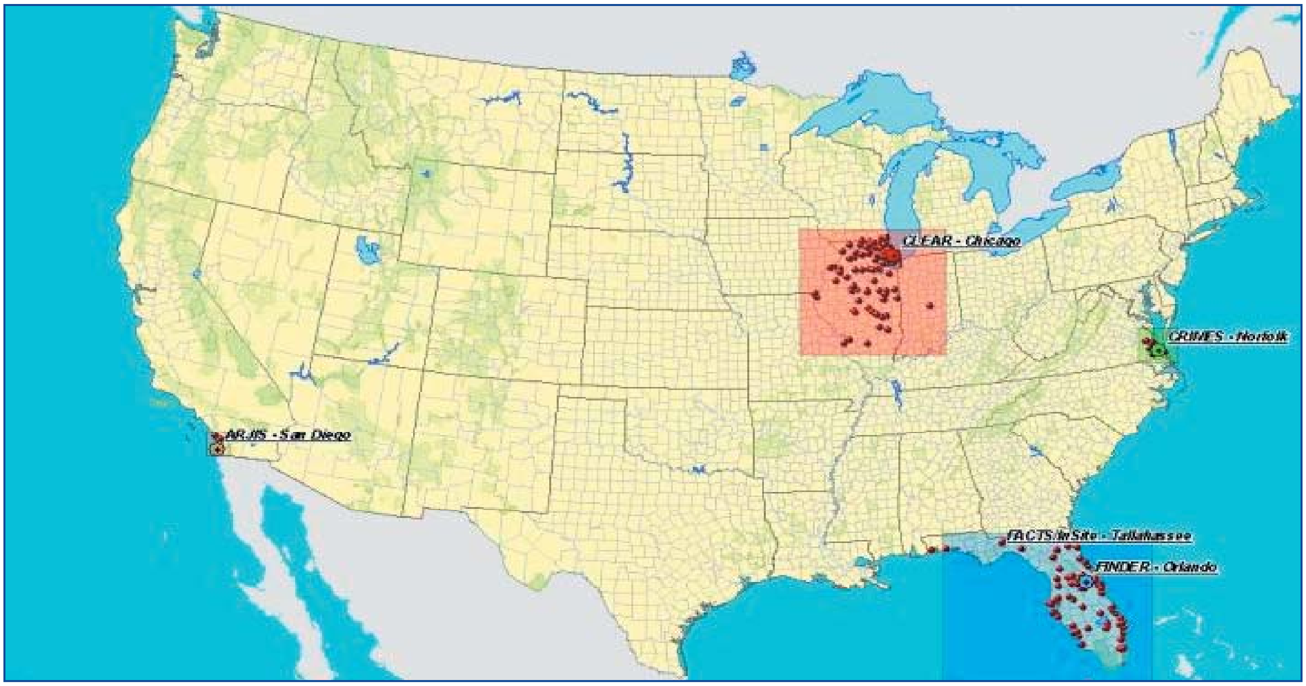


Figure 1-1. Overview Map of Surveyed Information-Sharing System Organizations

oped the following products to provide further information:

- **CRISP System Documents:** A system document was developed for each ISS interviewed. Each document provides detailed information on the governance, management, system architecture, and functional and technical capabilities of the ISS.
- **CRISP Mapping Application:** This application provides a visual means to view and compare information on the six interviewed ISSs.
- **Metrics for Law Enforcement Information-Sharing Systems:** This document examines the use of metrics as a tool to assess the effectiveness of a law enforcement ISS and its impact on operations.

The ultimate objective of CRISP is to develop the document, *A Practitioner's Handbook for Regional Law Enforcement Information-Sharing Systems: Preliminary Requirements*. The preliminary requirements document—based on the site visit interviews and analysis of the national survey results—represents a first step at defining functional and operational requirements for developing regional ISSs for law enforcement.

1.2 Purpose and Scope

The purpose and scope of this document is to describe the different approaches and methods found in operational systems for sharing law enforcement information regionally. The functional and technical characteristics and operational processes of the surveyed organizations are models of existing, mature regional information-sharing programs that have withstood reviews and growing pains. The best practices included in this document are intended to guide other law enforcement officials in their efforts to successfully implement similar systems.

The main portion of this document addresses the following topics as part of the CONOPS for an ISS that effectively shares law enforcement information among regional law enforcement agencies:

- Evolution and challenges of operational law enforcement information-sharing organizations
- Regional law enforcement information-sharing best practices
- Aspects of law enforcement operational procedures that benefit from information-sharing
- Approaches and methods used to share information

- Considerations that impact the success of regional information-sharing

1.2.1 Assumptions

This document assumes that the reader is a member of a law enforcement agency or government entity interested in the nature and structure of information-sharing practices among law enforcement agencies. The CONOPS described in this document originated from the needs expressed by surveyed law enforcement agencies and the best practices learned from agencies and organizations that operate the six ISSs that were interviewed and studied in depth. The principles discussed will remain valid even if the system-specific details change over time.

This document also assumes the reader has a basic understanding of technologies related to specific law enforcement applications, such as records management systems (RMSs) and crime analysis software. The reader is referred to the glossary for a listing of acronyms, abbreviations, and general terms relating to law enforcement, records management, and information exchange technologies.

1.2.2 Constraints

The information provided in this document reflects the input and experience gathered from interviewed and surveyed law enforcement agencies and operational law enforcement information-sharing organizations. All concepts, procedures, and specific system details were taken from published documents, user manuals, and other materials provided by the representatives of the information-sharing organizations. While many ISSs exist that include interfaces with other types of justice agencies, such as the courts, this effort focused on systems that support local and state law enforcement.

1.3 Structure of Report

The remainder of this document focuses on describing key areas of information-sharing and details on best practices for law enforcement.

Section 2 discusses the evolution, challenges, and needs associated with establishing an ISS for an organization. Section 3 describes the law enforcement information-sharing best practices identified through the on-site interviews and survey responses. Section 4 identifies issues and impacts associated with creating an ISS.

The document includes a set of Appendices. Appendix A provides reference information for data sources. Appendix B provides copies of the interview guide sheets used in Phase One of the data collection process, as well as blank copies of the national survey forms used in Phase Two. Appendix C describes the interview methodology that Noblis applied to the major ISS organizations. Appendix D provides a list of acronyms and a glossary of the terms used in this document and their context.

This page intentionally left blank

2 Information-Sharing: Evolution, Challenges, and Needs

This section describes the procedures used to establish operational information-sharing organizations and the challenges that have shaped their development. It also identifies the types of law enforcement information that is shared with and without an ISS. The section concludes with a discussion of the need for sharing this information and the users and work processes involved in an ISS.

2.1 Transitioning Toward Regional Information-Sharing

Today, law enforcement agencies depend on modern information technology (IT) to increase agency effectiveness and officer safety. Jurisdictions recognize the critical need for daily interagency information-sharing, cooperation, and communication. Of those interviewed, some operational ISSs started as early as 1999, which indicates the value of sharing information has been recognized in the law enforcement community for some time. Recognizing the cross-jurisdictional nature of criminal activity and increased post-9/11 attention on law enforcement interoperability, many police chiefs and sheriffs have come to understand that they need to improve their regional information-sharing capability. They see participation in a regional ISS as having two benefits, which were verified by national survey responses: it enables agencies to respond more efficiently to criminal and public-safety incidents, and it facilitates the evolution of proactive strategies for preventing crime, reducing the occurrence of public safety incidents and building a robust community-oriented policing environment.

2.1.1 Federal Guidelines Encouraging Information-Sharing

Emerging national plans for information-sharing have also spurred efforts by law enforcement to form information-sharing programs. The May 2004 NCISP outlines steps and strategies for sharing intelligence information across federal, state, tribal, and local levels. Several of the agencies interviewed for CRISP support one or more of the *10 Steps toward the NCISP*, developed by the Department of Justice (DOJ). Specifically, the four steps below predominated:

- Connect to your state criminal justice network and regional intelligence databases and participate in information-sharing initiatives
- Partner with public and private infrastructure sectors
- Participate in local, state, and national intelligence organizations
- Access law enforcement web sites, subscribe to law enforcement listservs, and use the Internet as an information resource

The following examples illustrate how this guidance is reflected in the approaches used by four of the ISSs:

- **CLEAR:** The Chicago Police Department (CPD) partnered with Oracle Corporation to create CLEAR. The CPD provided the subject-matter expertise, process knowledge, and data guidelines to Oracle (who provided their technical services and products at reduced rates). CPD has several online websites for sharing law enforcement information with their local citizens; these websites demonstrate their innovative use of contemporary technologies.
- **FACTS:** Like CPD, the Florida Department of Law Enforcement (FDLE) had a similar arrangement with Seisent to develop FACTS. FDLE drove the Seisent development effort, with law enforcement users creating requirements for the developers. Through the Joint Terrorism Task Force centers, FDLE provides several other law enforcement agencies—such as the Federal Bureau of Investigation (FBI), the U.S. Marshals, and Immigration and Customs Enforcement (ICE)—access to FACTS.
- **FINDER:** The FINDER consortium partnership draws upon the public sector via its collaboration with the University of Central Florida. The FINDER consortium leveraged the University's Internet development skills and research capabilities to create and operate their information-sharing capability.
- **ARJIS:** In 2004, ARJIS merged operations with the San Diego Area Governments (SANDAG), which further enhanced the state and local partnership. Recently, ARJIS created a new Public Safety Committee that expands the management of ARJIS to include elected

officials and members from the public safety community. In addition, ARJIS includes federal law enforcement joint task force users from the FBI, the Drug Enforcement Agency (DEA), and ICE. In a similar manner to the CLEAR system, ARJIS shares information with the community via an Internet-accessible website. Citizens can view high-level crime maps and publicly available crime reports.

Based on the national survey data, Figure 2-1 illustrates that most law enforcement agencies are familiar with the regulations that have more direct impact on their daily operations. Secure transmission of data, privacy concerns, and 28 Code of Federal Regulations (CFR) Part 23 pertaining to intelligence data are fairly well understood, as well as the Law Enforcement Information Technology Standards Council (LEITSC) draft guidelines for Computer-Aided Dispatch (CAD) and RMS.

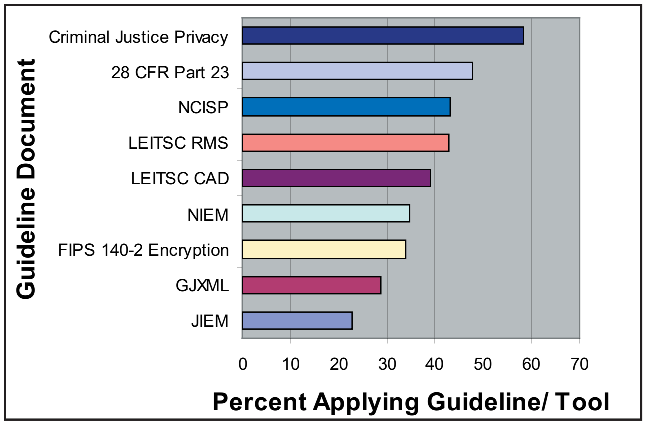


Figure 2-1 Law Enforcement Agencies Applying Information-Sharing Guidelines and Tools

2.1.2 ISS System Development Life Cycle

The interviewed organizations all followed iterative system development life cycles (SDLCs). A common theme of their operational development is the involvement of command-level staff and the user community to establish and prioritize the business needs and associated desired capabilities. *One key success factor is the active involvement of chiefs and sheriffs—or their representatives—in steering the information-sharing program from inception through all phases of development and operation.* This active participation ensures that the information-sharing program meets strategic agency needs and fosters active participation of agency staff in the design and development phases. Users collaborate with IT specialists to define the functional requirements of new features and to design the look and feel of such features as a new query, report, photo montage, or mapping capability. Users play key roles in operational testing as well; in some cases, new capabilities are initially rolled out to a designated group of users. Frequently, officers and analysts assist in the training of peers in their agency.

Rather than building all capabilities at once, most information-sharing programs have chosen to automate small components and then build upon those efforts to create a system. FINDER, CLEAR, ARJIS, and CRIMES all started development with small subsets of law enforcement data, such as pawn information and incident reports. Each program promoted an iterative SDLC approach for developing additional capabilities in their ISS. These SDLC approaches are variations of the DOJ SDLC illustrated in Figure 2-2. While some information-sharing programs (such as CLEAR) employ a more detailed spiral SDLC process, overall, the interviewed information-sharing programs recognized that certain phases of the SDLC—such as requirements analysis and joint application design (JAD) sessions—are critical to operational system development and are therefore considered a best practice.

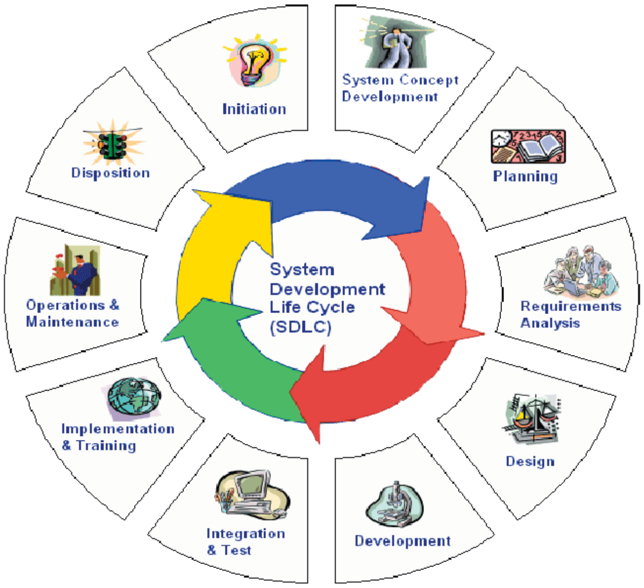


Figure 2-2 DOJ Systems Development Life Cycle Phases

Starting with the Initiation step, the interviewed ISS organizations all recognized the need for regional information-sharing through a local crime event or for compliance with legislative requirements. Organizations such as CRIMES, CLEAR, and FACTS invested a lot of time and resources into the system concept development, planning, and requirements steps to ensure user buy-in and functional needs. While these steps were critical to the process, the follow-on design, development, and integration steps were typically the main focus of time, cost, and personnel resources. Less time and funding was spent on the testing, training, and maintenance steps.

2.2 Challenges Encountered In Forming an Information-Sharing System

Groups that have attempted to form an ISS have faced a number of political, financial, and legal challenges. Often, efforts are hindered by factors that may seem to vary from region to region. This project found that there are common themes in the challenges and obstacles encountered by agencies when implementing a system to share law enforcement information regionally.

2.2.1 Organizational and Political Factors

Although the concept of sharing law enforcement information is not new, most of the established information-sharing occurs through personal relationships between officers in adjacent jurisdictions. Other instances of information-sharing occur in response to joint operations or on a case-by-case basis as needs arise. An ISS can bring a change of culture to a region as agencies now work as a team on crime resolution and prevention. Overcoming these established viewpoints and expanding the scope of information-sharing can be difficult.

Political impediments to information-sharing are a factor in all of the surveyed ISS organizations. Trust can be a major issue, for example, and can have an impact on how data owned and collected by one agency is viewed and used by another agency. If the ISS's organization is not structured properly, some police chiefs or sheriffs may refuse to join if their agency does not have an adequate voice on regulation and operational issues. Most of the major information-sharing programs also required the assistance of senators and congressional representatives. For example, CRIMES was established after Virginia Senator Charles Robb provided legislation that supported the creation of a law enforcement ISS supporting the Hampton Roads area. FDLE also received support from the Florida state legislature and legal authorization for operating ISSs.

2.2.2 Legal Statutes and Privacy Impact Assessments

Law enforcement information is bound by many legal constraints that vary from region to region. Most ISS organizations are encouraging agencies to share their data as long as the system users are sworn staff from member law enforcement agencies and such users are cleared to access the National Crime Information Center (NCIC) and state systems containing criminal history data. A common legal stipulation on regional ISSs is that they are not *systems of record*. A system of record refers to the originating or authoritative system source of data or information; systems that store copies of data or that store and retrieve data obtained from other data sources (such as an agency RMS) are not considered systems of record. If the ISS also functions as an RMS, then the system may be considered a system of record, as in the case of Chicago's centralized CLEAR system. In all cases, an investigator must check with the source agency to confirm a record's information before any of the information can support further action. Most ISSs also incorporate mechanisms to address Freedom of Information Act (FOIA) requirements regarding certain types of law enforcement records, audit logs, and other types of electronic storage media. This also applies to expungement of records.

ISS organizations recognize that the ISS must withstand the scrutiny of privacy advocates. For this reason, the regional data that is most commonly accessible is law enforcement information, such as incident, investigative, or field interview data. Some organizations have restricted the information they share to law enforcement information, specifically excluding intelligence information[3] and information from non–law enforcement agencies and commercial sources.

[3] The inclusion of intelligence data (e.g., non-factual data, suspicious activity data) may also require operating the system according to the operating principles defined in 28 CFR Part 23 or some other regulations depending on the funding source and agency policy for the handling of intelligence data.

In an effort to increase community trust and support, some information-sharing programs have performed privacy impact assessments. According to the International Association of Chiefs of Police's (IACP's) *Guidelines for Improved Automated Criminal History Record Systems and Effective Screening of Personnel,* there are four steps to follow when conducting a privacy impact assessment (see Figure 2-3). The four steps essentially take privacy regulations and policies and map the information-sharing processes against them to see if any violation or risk of misuse exists. The FDLE Office of Statewide Intelligence conducted a privacy impact assessment on the FACTS application in response to concerns about what data exists in the databases and whether the policies and procedures met the privacy requirements. By taking such action, FDLE documented what kind of information is and is not available in their ISSs. FDLE worked with the media and privacy advocates to alleviate privacy concerns and misconceptions on the law enforcement use of public data. ARJIS utilizes a privacy attorney who is consulted on all potential issues that arise pertaining to privacy concerns. The ARJIS Joint Powers Act is reviewed annually by legal staff to ensure that law enforcement is meeting the legal obligations involved in data handling and data access. Federal systems have similar privacy concerns and must abide by the February 2001 DOJ *Privacy Impact Assessments for Justice Systems* guidelines. The IACP guidelines reference the DOJ document, which provides some consistency between the federal and state perspective. Other interviewed ISS organizations recognize that performing a privacy impact assessment will be a key step for developing mature law enforcement ISSs. While conducting a privacy impact assessment is strongly recommended, there is no guarantee that the impact assessment will address all privacy concerns.

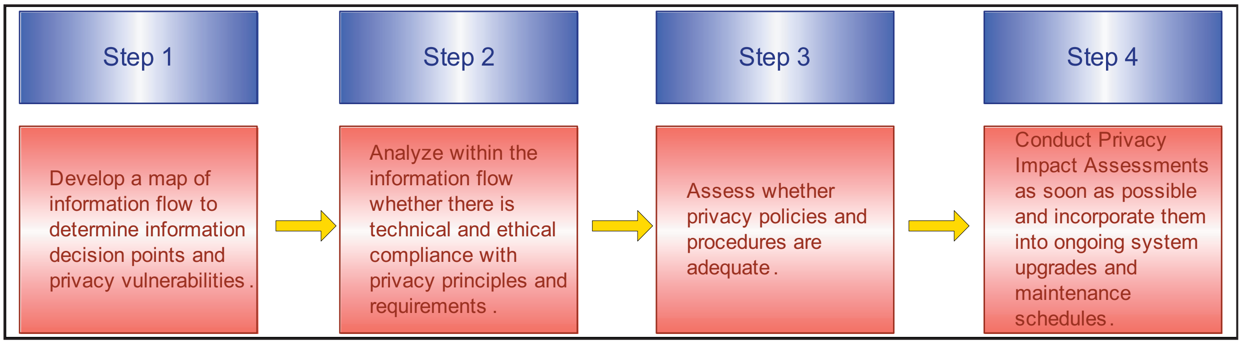

Step 1
Step 2
Step 3
Step 4
Develop a map of information flow to determine information decision points and privacy vulnerabilities.
Analyze within the information flow whether there is technical and ethical compliance with privacy principles and requirements.
Assess whether privacy policies and procedures are adequate.
Conduct Privacy Impact Assessments as soon as possible and incorporate them into ongoing system upgrades and maintenance schedules.

Figure 2-3 IACP Privacy Impact Assessment Steps

In addition to privacy impact assessments, some organizations implemented other measures to show how the ISS benefits and supports the public. CPD has several outreach measures for gaining trust with the public, such as a web site for citizens to see maps of where crime is occurring in the city. ARJIS and FINDER also provide public web sites that supply useful information for area residents. Other organizations have formed a close relationship with their state legislatures. For example, FDLE has collaborated with the state legislature so that the enacted laws and the systems developed to support the laws are in concert. CPD has worked with their Legal Affairs on rulings on electronic signatures and court consent decrees related to gang information.

2.2.3 Funding Sources

Financing an ISS is a major issue for law enforcement agencies. Many of the existing ISS organizations required a large, initial funding source to establish the governance body, policies, and personnel. This funding also supported establishing the required interconnections for sharing information with other agencies. Once the initial funding source was exhausted, other funding sources were solicited to maintain operations and implement enhancements. Financial management is frequently a complex and time-consuming task that should not be underestimated and may require more effort than can be performed by a person with other full-time responsibilities. The funding paradigm took several forms:

- **Federal Grants:** Funding awarded through grant applications for specific programs has helped organizations link efforts and systems together to form an ISS. Although the grants targeted specific crime areas and applications, the grants provided a forum for adjacent agencies to meet and share information. Example grant programs include the Office of Community-Oriented Policing Services (COPS) Making Officer Redeployment Effective (MORE) grants and region-specific funds through the DOJ. CLEAR and FDLE leveraged funding from both programs to develop portions of their ISSs. ARJIS started with a federal grant from the NIJ. Since that initial funding, ARJIS has shifted to a 100 percent membership-supported cost structure. As previously noted, CRIMES received congressional funding from Virginia Senator Charles Robb. Table 2-1 clearly shows that federal funding was a common component in the evolution of the interviewed ISS organizations.

Table 2-1 ISS Funding Sources

ISS	Federal Grant	State Funding	Local Budgets	Mutual Aid
CRIMES	✓	✓	✓	
ARJIS	✓		✓	✓
FINDER	✓		✓	
InSite		✓		
FACTS	✓			
CLEAR	✓		✓	✓

- **State Funding:** Funding through state governor offices and state legislatures has also assisted agencies in their information-sharing efforts. CRIMES received a state grant that required agencies to match a portion of the grant. The Florida legislature authorized development of FDLE's FACTS and InSite through legislative bills.
- **Local Budgets:** Towns and cities have formed consortiums or signed Memoranda of Understanding (MOUs) and devised funding formulas to pool resources for establishing an ISS and more commonly, for sustaining ISS operations and future enhancements. The CPD is a prime example of an agency that funded CLEAR through their budget cycles. The most common funding formula—used by FINDER and CRIMES—is a sliding-scale fee based on the number of sworn officers in an agency. Member agencies at both organizations found this approach more equitable than one based on population.
- **Mutual Aid Agreements:** Traditionally, mutual aid agreements have formed the basis for organizing investigative teams or task forces. Regional mutual aid agreements can include provisions to meet specific needs, address likely threats, and make available the full range of existing resources.[4] These agreements can also play a role in regional information-sharing when they are used to define how an agency will contribute funding or staff resources to an ISS. For the CPD, the Cook County Sheriff's department invested local funds into CLEAR after seeing the benefits from using the system. Other agencies, such as the San Diego Police Department, work with ARJIS and surrounding agencies to provide support to the ISS. Each agency allocates resources independently and contributes in-kind services based on their relative strengths.

2.3 Law Enforcement Information-Sharing

This section discusses the types of law enforcement information shared in a traditional, non–information-

[4] From *Mutual Aid: Multi-jurisdictional Partnerships for Meeting Regional Threats* by Phil Lynn, IACP September 2005.

sharing program agency setting versus how information is shared among ISS participants. The surveyed information-sharing programs all use automated information systems that authorized member agency staff can access via secure links from their desktop computers and, in some instances, from mobile data terminals or wireless handheld devices.

2.3.1 Traditional Information-Sharing Models without an ISS

Without an ISS, most law enforcement agencies operate according to the classic police functions associated with preventing, monitoring, and solving crime. Departments within agencies can sometimes operate independently with limited sharing of information. In this setting, most of the information-sharing occurs based on personal relationships and whether other personnel are aware of an ongoing investigation. Telephone calls, physical trips to records departments, and faxes or emails are common methods of sharing information without an automated ISS. Before CLEAR, detectives in the CPD recall having to wait hours for case record files, photo montages, and validation of information from the central records department or other areas in the city. Agencies without an ISS deploy their tactical teams based on field reports and officer observations on crime in their jurisdiction. Patrol officers without access to a regional ISS rely heavily on the dispatcher to check station records for suspect information. Table 2-2 shows a list of information types and the mechanisms used by agencies to share such information without a formal ISS.

Table 2-2 Information Shared in Non-ISS Agencies

Information Type	Sharing Mechanism
RMS data files, photos	Email messages and attachments
Incident, arrest, warrant data	Phone calls/meetings
BOLOs, citizen bulletins	Facsimiles/mailed documents
Field interview/pawn slips	Physical case files/ personal contact

2.3.2 Information-Sharing with an ISS

Interviewed information-sharing representatives ranked the types of information shared by the order of importance to law enforcement. Those interviewed identified the most needed types of information—information that would assist in positive identification of suspects, the history and names of individuals associated with an address, and vehicle information obtained from partial vehicle information searches. Based on these needs, photos, arrest reports, and incident reports are the highest priority for sharing among agencies. Other information, such as pawn data, was identified as valuable but was not considered critical. Field interview reports are likewise highly desired, but they—along with pawn slips—are not typically captured in an automated fashion.

Figure 2-4 illustrates how most ISS organizations have focused on sharing arrest reports, incident reports, and photos (typically from mug shots but also from driver's license photos). Many automation efforts have focused on transforming these items into an electronic form. Based on the interview information, agencies in an ISS more readily share electronic forms of data versus paper reports. After developing an initial sharing capability, many ISS organizations will realize the need for more analysis tools, moving beyond simple

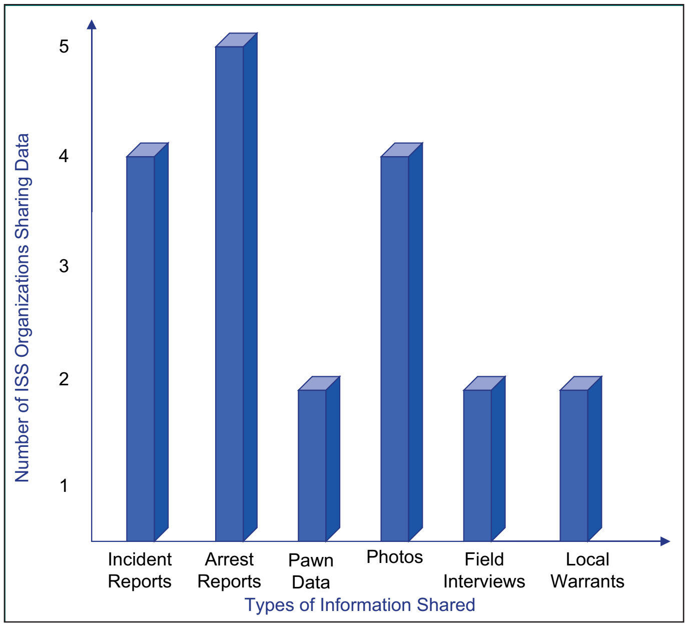


Figure 2-4 Number of ISS Organizations Sharing Data Type

record checks and searches. The focus changes to creating links among the disparate pieces of information to generate leads and correlations.

Those interviewed said that it would be desirable to expand the amount of information available electronically by increasing the amount of field interview, traffic accident, and pawn data. This information was considered valuable for improving the ability to identify suspects, locate known criminals or recidivists, and establish crime patterns on a regional basis. Table 2-3 shows how, for ARJIS, the emphasis is on criminal cases and arrest information. Percentages vary among the systems; for instance, FINDER started operating with pawn-related data. The electronic pawn information has provided key links between stolen property and suspected individuals.

Table 2-3 Percentage of Data in ARJIS

Data Type	Percentage in ARJIS
Criminal Investigative Cases	49%
Arrest Reports	21%
Traffic Citations	9%
Field Interviews	5%
Traffic Accident Reports	6%
Pawn Slips	9%
Forges Documents	1%

Source: *IACP An Information Integration Planning Model, April 2000*

Another common theme cited was that the more current the data, the more useful it is. One positive impact of information-sharing programs is that in addition to saving time in obtaining access to data (e.g., arrest records or mug shots available by the entry of a query rather than driving across town), the data in the ISS is frequently available shortly after capture, meaning that the data is very current. This is the case when there are capabilities for automated data entry (e.g., arrest records in CLEAR) coupled with an ISS capability to gain access to that information in a matter of hours. Most ISS data is typically updated every 24 hours; whereas in some systems, such as CLEAR, certain data is updated every six hours.

2.4 Law Enforcement Information-Sharing Needs

Law enforcement agencies that have shifted their view of crime from a local to regional perspective are forming regional information-sharing programs. Agencies without an ISS have local information needs, goals, and processes that focus on traditional law enforcement functions. The following sections discuss the goals and user roles typically found in law enforcement agencies that are not participating in a regional automated ISS.

2.4.1 Non-ISS Law Enforcement Agency Information-Sharing Goals

Over the past 200 years, law enforcement agencies have realized the need for sharing information, primarily among internal police units. These information-sharing goals address various areas, such as terrorism prevention, drug enforcement, and public awareness. Table 2-4 lists some of the information-sharing goals from police departments around the nation. This data is taken from agency web sites outside of the CRISP survey effort.

There are several examples of agencies implementing efforts to support these goals. The Sheriff’s Office in Oakland County, California, uses online maps and “most wanted” profiles on their public website to share information among departments, as well as with the public. Agencies such as the Police Department in Troy, Michigan, have been using email to notify residents, businesses, and community groups about recent crime incidents in their areas. Other agencies—such as the towns of Bladensburg and Mount Rainier in Maryland—established a shared dispatching and code system. As mentioned in Table 2-4, Nassau County (New York) formed a partnership between law enforcement and the private sector to identify and discuss crime trends and solutions. SPIN members use meetings, email, and text notifications to share information regarding recent bank robberies, explosions, and other incidents. Other efforts like SPIN exist that rely on in-person meetings for sharing information.

Based on the national survey data, Figure 2-5 illustrates that law enforcement agencies that have not participated in an ISS want to share all forms of data possible.

Table 2-4 Examples of Information-Sharing Goals from Agencies Not Participating in an ISS

Information-Sharing Goal	Agency
“The agency must seek to collaborate with neighborhoods to better understand the nature of local problems and to develop meaningful and cooperative strategies to solve these problems.”	Fairfax County, Virginia Police Department
“Maintain a safe environment for all citizens and aggressively address criminal activity throughout the City by developing partnerships throughout the community. Maintain a low crime rate. Integrate proactively with other departments/agencies.”	Kansas State Police
“The goals of the Security Police Information Network (SPIN) are to share information, identify and discuss crime trends and solutions, work together toward the common goal of protection of persons and assets. SPIN creates a better working relationship between law enforcement and the private sector.”	Nassau County Police, New York

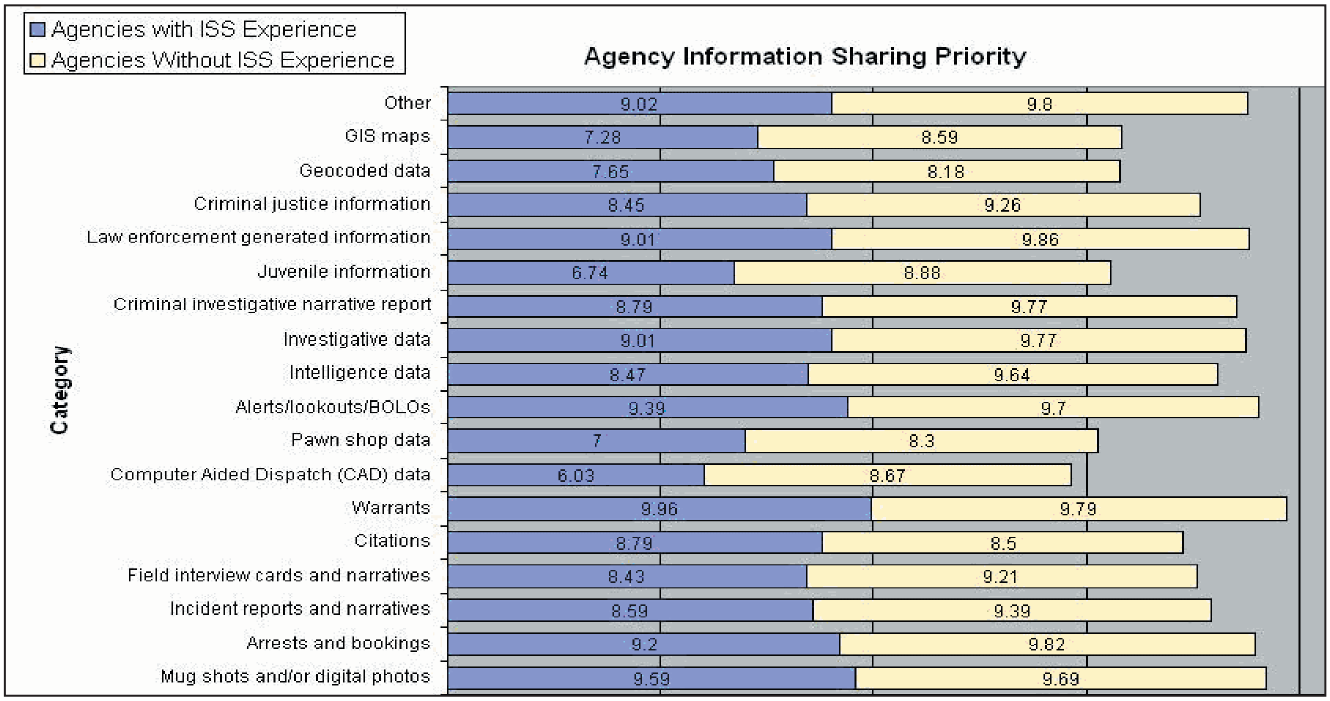


Figure 2-5 Agency Information-Sharing Priority

The results (scaled 1 to 10, with 10 indicating information considered most useful) show that the experienced agencies recognize what categories of data are the most useful and practical to share. Agencies experienced in ISSs ranked the priority of sharing information differently in a few areas. Sharing CAD data was not a highly ranked category by agencies participating in an ISS even though non-ISS agencies gave this function a high rating. Similarly, juvenile information was not a high priority to the ISS agencies versus the non-ISS agencies. The survey data affirmed that the most sought after data categories by both groups were mug shots, digital photos, warrants, arrests and bookings, and lookout information (BOLOs). The “Other” category in Figure 6 refers to driver’s license and vehicle registration information, which were rated highly by both groups.

2.4.2 Work Processes: User Classes and Descriptions

Agencies who do not participate in an ISS have defined business processes for performing their law enforcement functions. The following user group descriptions represent how traditional law enforcement roles could benefit from the formation of an ISS.

- **Decision Support:** Command staff typically retains full access control for performing auditing, approval, and review functions. The command staff does not typically enter data or perform in-depth analysis on daily tactical data. This group focuses on strategic decisions, implementing proactive crime prevention measures—such as those involved with patrol deployment—to meet the needs of the community.
- **Administrative Support:** Administrative staff support command staff by running the operational and information management systems. Many agencies possess some level of automation for collecting, searching, and storing information. Staff may also have administrative-level access even though they do not perform command staff duties.
- **Detectives:** Officers that investigate crimes and cases develop sources of information and locate and interview confidential informants. Some of the specialized duties performed by a detective include conducting narcotics investigations, performing surveillance, establishing and maintaining contacts with informants, investigating gang-related crimes, responding to and investigating crime scenes, and identifying suspects.
- **Crime Analysts:** Crime analysts study crime incidents that have occurred and profile suspects. They analyze crime data to identify crime patterns, track the level of criminal activity, and determine the impact of crime prevention efforts. Crime analysts communicate crime patterns to command staff, detectives, and patrol officers to support efficient deployment of law enforcement resources. Three types of crime analysis are used by crime analysts:
  - **Tactical:** Detect a pattern from crimes by studying and linking common factors together such as method, suspect physical description, and weapon used
  - **Strategic:** Provide strategic information that enables command staff to deploy resources where police presence needs to be increased or decreased or for initiating special operations
  - **Administrative:** Provide special reports to police chiefs and city councils that interpret crime statistics categorized by factors such as

  graphical locations and economic conditions

  For each analysis type—and in order to plot suspect activity—the crime analyst scrutinizes daily crime data that enters the police agency through the various types of police reports that are completed, such as incident reports.
- **Intelligence Analysts:** Intelligence analysts study criminal relationships and suspicious activities to link suspects to criminal organizations or events. They also focus on organized crime, such as narcotics smuggling, money laundering, gangs, terrorism, and auto-theft rings. Intelligence analysts work with officers who gather information by field observation, confidential information sources, and public records. Intelligence analysts serve additional functions, such as the following:
  - Establish criminal profiles that include prior crimes and criminal relationships to aid in making a connection between members and the organization
  - Use telephone toll analysis to plot telephone activity to determine the size and location of criminal groups and individuals involved
  - Study suspects' assets to determine the flow of money going into and coming from a targeted group
- **Patrol:** Patrol officers respond to calls for service, identify suspects, and gather any known history on persons, places, or vehicles. Job functions include conducting searches of people, vehicles, buildings, and outdoor areas that may involve interviewing people, detaining people, and stopping suspicious vehicles and persons.

This page intentionally left blank

3 Information-Sharing Best Practices, Work Processes, and Metrics

This section describes specific governance and management practices that support regional law enforcement information-sharing. These practices affect operations, maintenance, and training, as well as other system support required to deploy and operate the ISS. This section also includes functional best practices as observed at the six surveyed sites.

3.1 Goals and Objectives

A first step for any group interested in forming a regional ISS is to establish goals and objectives that support the information-sharing program's mission statement. These goals and objectives form the vision that drives the needs and ISS operational structure. The set of objectives then define measurable tasks for progressing toward achieving each goal. Figure 3-1 shows how goals are supported by objectives, strategies, and operational tasks.

ISS representatives had different definitions for what was a goal versus an objective. An objective found in one ISS may translate to a goal in another ISS. Please refer to the corresponding system document for a better understanding of the evolution of the goals and objectives for a particular ISS. The following sections present example goals and objectives based on documentation and interview responses.

3.1.1 Information-Sharing Goals

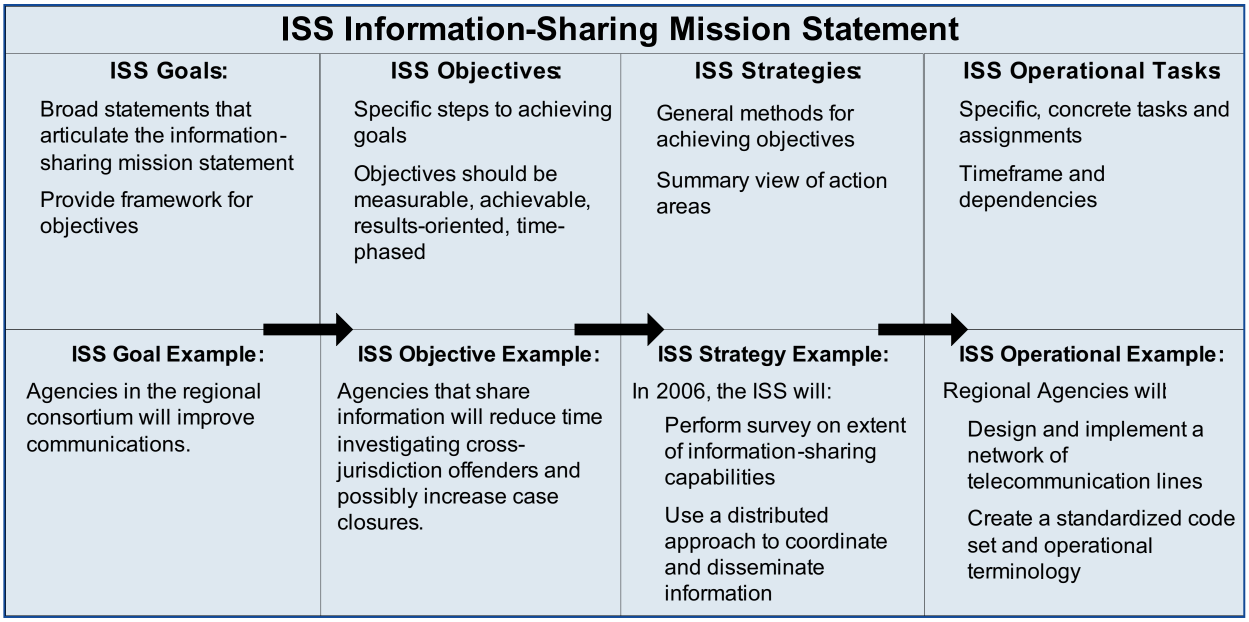
As a best practice gleaned from interviewed ISS personnel, the goals of ISS organizations consist of broad statements that articulate the information-sharing mission statement. The discussion in this section illustrates goals formed by the interviewed ISS personnel.

3.1.1.1 Example Governance Goals

A strong management structure with a clear set of goals is a key factor of any operational ISS. The law enforcement management goals center on interagency communication, personnel, and resource control issues. Other areas include officer management and accountability, standards compliance, and improved tactical and strategic planning capabilities. As Table 3-1 shows, management goals should provide broad statements that set the framework for the objectives.

3.1.1.2 Example Goals for Information Dissemination Among Law Enforcement Agencies and With the Public

Additional goals involve the access, sharing, accountability, and analysis of ISS information. The sensitive nature of law enforcement information requires secure



ISS Information-Sharing Mission Statement

ISS Goals:	ISS Objectives:	ISS Strategies:	ISS Operational Tasks
Broad statements that articulate the information-sharing mission statement Provide framework for objectives	Specific steps to achieving goals Objectives should be measurable, achievable, results-oriented, time-phased	General methods for achieving objectives Summary view of action areas	Specific, concrete tasks and assignments Timeframe and dependencies
ISS Goal Example:	**ISS Objective Example:**	**ISS Strategy Example:**	**ISS Operational Example:**
Agencies in the regional consortium will improve communications.	Agencies that share information will reduce time investigating cross-jurisdiction offenders and possibly increase case closures.	In 2006, the ISS will: Perform survey on extent of information-sharing capabilities Use a distributed approach to coordinate and disseminate information	Regional Agencies will: Design and implement a network of telecommunication lines Create a standardized code set and operational terminology

Figure 3-1 Policy Structure Supporting Information-Sharing Goals

Table 3-1 ISS Governance Goals Based on Available Data

Originating ISS	Governance Goal Statement
ARJIS	We use information technology in coordination with community partners to proactively address community concerns.*
ARJIS	The San Diego region provides its officers with state-of-the-art information technology that enhances both officer and public safety.*
CRIMES	Facilitating communications among participating agencies.
CRIMES	Support all aspects of the criminal justice process through automation.
CLEAR	CLEAR is expected to promote effective resource allocation; officer management and accountability; risk management and early warning; tactical and strategic planning; and fiscal accountability.
FINDER	Secure and credible data interoperability among Florida law enforcement agencies to assist with domestic security initiatives and crime control in a timely and effective manner.**

*From the *2003 Final ARJIS/SANDAG Consolidation Plan* **From the *May 2005 Presentation of FINDER Objectives*

methods and policies for its sharing and handling. All of the organizations interviewed have indicated that shared records are not the official record and investigators must verify the lead information with the originating agency. Sharing information with the public is another key goal to building trust between the public and law enforcement. It also helps the public gain an understanding of why information-sharing among agencies benefits their safety. Table 3-2 offers goal statements for information dissemination; these goals reflect a focus on improving information dissemination, improving the gathering of information, and providing other criminal justice users with timely, accurate law enforcement information.

Based on the national survey data, Figure 3-2 illustrates that law enforcement agencies see that information-sharing helps the most with local crime solving, local crime prevention, and community relations. These results fit in with the local agency focus on solving crimes within their jurisdiction. Sharing information for drug and crime task force activities is also ranked high since most, if not all, jurisdictions have some activity occurring. The local law enforcement agencies along major transportation corridors such as Interstate 5, 66, and 95 have long recognized the importance of information-sharing as they track the movement of criminals and illegal drugs across the nation. Assisting federal and state task forces is seen as a lower priority since it may not concentrate much on the local issues.

Table 3-2 Information Dissemination Goal Statements

Originating ISS	Information Dissemination Goal Statement
ARJIS	We are committed to a collaborative agreement which includes public/private partnerships and federal, state, county, a municipal public safety agencies.*
CRIMES	Provide information to analysts, investigators, command staff, patrol officers, and dispatchers within their local region as well as users from federal and other jurisdictions.
CRIMES	Establish a formal communications network among all Participating Jurisdictions.
CLEAR	Strengthen problem-solving capacity; conduct community-needs assessment; and allow for easy and convenient information-sharing and intelligence gathering from community.
CRIMES	Provide information required by other agencies (state/federal) through automated interfaces.

*From the *2003 Final ARJIS/SANDAG Consolidation Plan*

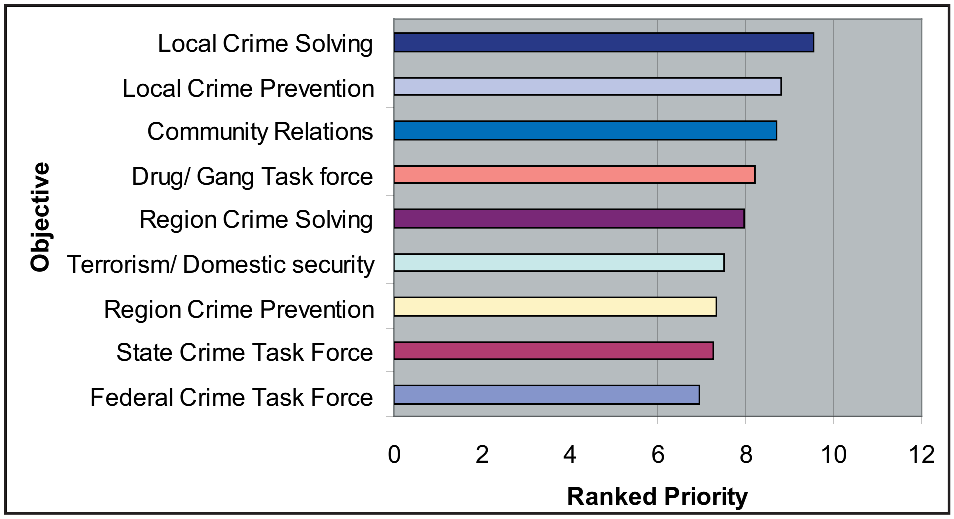


Figure 3-2 Objectives of Information-Sharing

3.1.2 Example ISS Objectives

Objectives vary to a large extent based on the particular needs and functions of the ISS. As they address more tactical-level issues, ISS objectives focus on shorter-term problems and projects that work toward supporting ISS goals. Unlike goals, objectives are precise, tangible, and concrete. Typically, objectives include specific dates, program names, and vendor products, among other details, while goals do not involve specifics. A schedule can map out the tasks required to fulfill the objective, such as implementing a new work process or vendor product by a deadline. If the tasks are not completed by the set timeframe, then the objective is not met. Some ISS efforts started without a formal set of declared objectives, while others revised their objectives as the ISS capabilities evolved.

Table 3-3 shows example objectives from some of the surveyed ISS organizations. The top three objectives observed are summarized below:

- Reducing the time spent searching for data
- Increasing the number of available information sources
- Having modern technical tools linked to reduce data-entry redundancy

Table 3-3 ISS Objectives Statements

Originating ISS	Objective Statement
ARJIS	Obtain information on problem area prior to or while on patrol
CRIMES	Reduce data entry redundancy
CRIMES	Provide information required by other agencies (state/federal) through automated interfaces
CRIMES	Improve efficiency and effectiveness of criminal justice agencies by providing access to accurate, dependable, and timely information
CRMES	Develop a regional criminal justice information system utilizing current technology and tools which will facilitate keeping the system functioning at a level that continues to meete the needs of the criminal justice user environment
FINDER	Creation of an open architecture infrastructure based upon national technology standards, which will enhance interoperability and information-sharing statewide

3.1.3 Metrics and Measures of Effectiveness

To date, there is no established set of metrics for regional law enforcement ISSs. The metrics commonly collected and reported cannot substantiate the effectiveness of ISSs or expenditures related to providing a specific feature or access to another data source. Most ISS organizations collect system uptime, network bandwidth, and database allocation utilization data. While these statistics are useful for daily operations, the metrics do not necessarily help determine how effectively a system meets law enforcement needs. A set of metrics would help information-sharing organizations quantify and qualify the level of effectiveness gained through the use of their system.

All of the ISS organizations attempt to capture information from their users via interviews, user feedback from built-in system mechanisms, and success stories of how the system aided case closures. For example, FINDER is revising its ability to capture success stories to enable a user to select specific categories that describe how the system supported the user to reach a conclusion. This is being implemented as a means for developing a first set of metrics.

One common theme expressed was that analysts could not do their jobs without access to the ISS and a number of other systems that they use on a daily basis. The most common theme involved examples of time savings by the automation of previously manual tasks (such as providing a query capability that eliminates the need to drive across town to get an arrest record).

Another common theme was that analysts wanted the system to provide known associates for a person of interest. Systems such as FACTS would provide investigators additional leads on casual links formed through field interviews, traffic tickets, or other collected data. From a site survey, an investigator described how the landlord of a former subject's address identified the subject's girlfriend. Locating the girlfriend led investigators to the subject's present location. Such leads from the ISS would provide investigators more options in reducing the time needed to close active cases.

Unique ways of correlating data that enhance effectiveness and intra- and interagency collaboration were also discussed. One example of such collaboration may be the use of the ISS to determine arrestees who reside in one jurisdiction, but are arrested in another jurisdiction. Likewise for offenders, suspects, or associates residing in one jurisdictions and are named in incident reports for another jurisdiction. Another example is pawn detectives using FINDER to identify individuals on house arrest who had performed a pawn transaction in a pawn shop. The detectives soon began collaborating with the home arrestee program officials. Collecting metrics related to these types of collaborations, and others, depict the many ways an ISS may be used to share information and to determine the need for an information sharing tool.

In another example, patrol officers handling traffic incidents used ARJIS to determine which intersections were the most frequent sites of traffic accidents. Officers were able to have their counterparts in another agency change the traffic signs and signals at the intersection, which resulted in a subsequent decrease in traffic accidents at the intersection. The CRISP team also observed how motorcycle officers in the city of Escondido's Police Department used their handheld devices to run vehicle plates and identity checks from traffic stops.

Many examples of strategic deployment were provided, such as the CPD Deployment Operations Center, which was started because of the availability of the extensive data analysis capabilities of the CLEAR system. ARJIS federal users also discussed how they used ARJIS on surveillance and how they shared photos and identification information with other team members coming on shift—information that might be critical to an officer's safety and effectiveness. InSite investigators and analysts were able to de-conflict cases so that an agency working on a particular case would know to contact another agency that may have information on a person of interest or an active ongoing operation.

From research conducted for CRISP, it is evident that the establishment of a metrics program should be one of the early objectives of an ISS organization. The goal of a metrics program should be to identify objectives that can be measured to provide both objective and subjective measures of success and effectiveness. These metrics and evaluation factors will both justify the existence and continued operation of the ISS and identify what works, what does not work, and what features are desirable but not worth the investment.

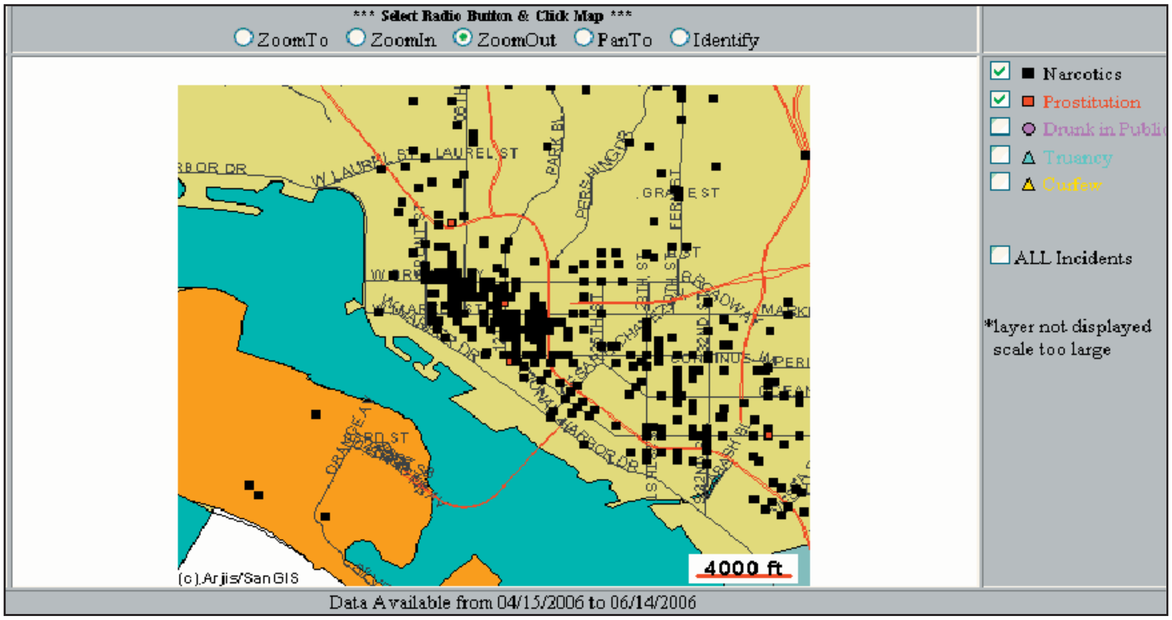
This subject is discussed in detail in the CRISP companion document, *Metrics for the Evaluation of Law Enforcement Information-Sharing Systems.*

3.2 Work Processes: User Group Descriptions

While each ISS organization has its own characteritics and unique capabilities, end users fit into a set of general categories that reflect their functions and level of information access. Each group of users has a key role in the ISS process, where some user groups rely on others for information. The following user group descriptions reflect how implementing an ISS affects user roles:

- **Decision Support:** The command staff typically retains full access control for performing auditing, approval, and review functions. Command staffs participate on the information-sharing governing bodies to oversee any contractors, provide the guiding decisions in developing functions, and establish system policy. Command staff may use the reports or results of ISS data analyses to implement special deployments in response to identified crime patterns, to initiate a crime prevention strategy, or to enhance the community-oriented policing capabilities of the agency. Command staff may also incorporate use of ISS data to augment their agency's COMPSTAT[5] program.
- **Administrative Support:** The administrative staff supports the command staff by running the operations and information systems of the ISS. They often also have administrative-level access, but they cannot typically perform command staff duties.
- **Investigators:** These officers use the ISS to develop sources of information and to locate confidential informants for interviews. The ISS provides investigators with the tools for linking people, places, and vehicles with much less labor when compared to the manual process. The ISS provides more leads because cases now have information from other agencies that was difficult to access before the tools existed. In addition, links can be established between entities that were not possible previously in the same timeframe.

[5] COMPuter STATistics, developed by the New York City Police Department, is used to manage and analyze crime trends. COMPSTAT employs Geographic Information Systems geo-coded data to map crime, detect patterns and hot spots, and devise strategies and tactics to solve and reduce crime (see Figure 3-3).



*** Select Radio Button & Click Map ***

○ ZoomTo ○ ZoomIn ● ZoomOut ○ PanTo ○ Identify

☑ ■ Narcotics

☑ ■ Prostitution

□ ● Drunk in Publi

□ △ Truancy

□ △ Curfew

□ ALL Incidents

*layer not displayed scale too large

Data Available from 04/15/2006 to 06/14/2006

Figure 3-3 ARJIS Crime Map Excerpt Showing Area Incidents

- **Crime Analysts:** Based on this research effort, crime analysts are the heaviest ISS users for their functions. Unlike patrol officers, an analyst's role is to research and link pieces of information into a case for follow-up by the detectives and patrol officers. Forming an ISS increases the amount of data available to crime analysts, which improves their ability to develop crime patterns, track movements of wanted individuals, and possibly identify more leads with the goal of closing more cases than in the past.
- **Intelligence Analysts:** Intelligence analysts receive a similar benefit as the crime analyst when they use an ISS. The ISS may be used in addition to other disparate intelligence sources to check for suspicious activity linked to potential terrorist activity. CRIMES intelligence analysts use their ISS for drug enforcement support and for background information for Customs seizure operations. The analysts are frequently asked by a network of intelligence analysts from other agencies to use the ISS to develop leads for their cases; as a result, an ISS can increase collaboration on the sharing of intelligence information beyond the region in which it operates.
- **Patrol:** For most ISS organizations, the patrol officers have limited access to the regional system. Most of the patrol officers who do use the ISS mainly focus on identifying suspects and gathering any known history on persons, addresses, or vehicles. Patrol also can indirectly benefit when dispatchers have access to the ISS and can handle more detailed inquiries, which can then return more and better information to the patrol officers. Supervisors also provide patrol officers with information from the system on suspects, drug areas, and vehicle photos that officers may encounter while on patrol.

3.2.1 Perceptions of Regional Information-Sharing Systems

Although there are many advantages cited for using an ISS, the interviewed ISS representatives noted that not all officers and detectives come to rely on the ISS for solving crimes. According to a study conducted by Dr. Martin Zaworski,[6] a law enforcement agency not using an ISS had the same violent crime case closure rate as did a law enforcement agency with access to ARJIS. The same study also noted that for property crimes, the non-ISS–equipped group cleared almost triple the number of cases versus the group with ISS access.

As might be expected, however, interviewees of ISSs containing regional Pawn data—such as FINDER—consider the system invaluable in solving property crimes; the FINDER program has collected numerous success stories to that effect. Similarly, lead generation of subject associates and addresses with systems such as FACTS, CLEAR, and ARJIS were cited as being critical to solving cases.

Officers appear to view automated ISSs as tools that require time and skill to use effectively, and interviewees noted that the systems are of the greatest benefit to the analyst and investigator—the "power" users. Mentoring by key "power" user peers was observed as being a factor in system acceptance. At the time of the CRISP interviews, several of the ISSs were not commonly being used directly by street-level officers although interviewees noted that dispatchers and investigators sometimes provide officers with information obtained from the ISS. On the other hand, interviews with ARJIS and FINDER users included street level "power" users who find the system invaluable in their jobs.

Some officers who used ARJIS stated that they experienced information overload and could not quickly decipher the key elements needed to take action. Such differences in the acceptance of an ISS come about as a result of many factors, including the user's level of familiarity with modern technology. The interviewees noted that often younger staff and those who commonly use the Internet for Google searches are more apt to use an ISS effectively and come to rely upon it. Training was noted as another factor that influences ISS use.

[6] Zaworski, Martin J. *Assessing an Automated Information-Sharing Technology in the Post '9-11' Era: Do Local Law Enforcement Officers Think It Meets Their Needs?* January 2006

3.3 ISS Functional Best Practices

This section describes the best practices observed in the functional capabilities provided by interviewed ISS personnel.

3.3.1 Types of Queries

One of the major capabilities provided by law enforcement ISSs involves the types of queries available for use. Information typically requested by law enforcement centers around three areas: people, locations, and vehicles. While different ISS organizations vary in their definition of these three areas, a core set of data is typically associated with queries performed for each type of information. Table 3-4 provides a brief overview of the three query categories and the data fields typically associated with each query type.

Based on the interviews of the ISS representatives, users most often query for person-related data. This anticipated result ties back to the duties performed by patrol officers when enforcing safety regulations and investigators when investigating a crime. Table 3-5 shows sample query types and whether an ISS offers that query capability based on the information collected from the site interviews. Extending the analysis to other ISS organizations through the national survey results, Figure 3-4 shows that the trend continues with the emphasis on identifying people and finding the history associated with a particular individual.

Although agencies are primarily interested in cases within their own jurisdictions, agencies on the border of major metropolitan areas and agencies joined by interstate highways often have problems that affect the entire region. Many ISSs have established data extraction or collection mechanisms, but few have moved forward with the advanced linking of related data. For several of the ISS organizations, moving past the data collection stage into the use of analysis tools that can identify and illustrate cross-border activities will be the next step in sharing information.

3.3.2 Analytical Capabilities

A major advantage for law enforcement agencies participating in an ISS is the ability to 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. The six surveyed ISSs all have reporting and querying capabilities as discussed in the previous section. This section examines which analytical tools and capabilities the ISS organizations have and which future features would prove the most useful to reducing crime.

The focus on data collection is now shifting to data analysis as many organizations have either too much data or no means of linking valuable data elements together in a timely fashion. Due to cost and complexity, ISS organizations have only recently begun trial test use of advanced analysis tools on the ISS data. Many sites rely on the querying and reporting capabilities to produce tabular results that analysts then manually process. Before applying analytical tools to the ISS data, ISS organizations recognize that they need to improve the quality, accuracy, and timeliness of the data entered. Table 3-6 shows how several types of analytical capabilities and sources vary from system to system.

The more established ISS organizations—such as ARJIS and CLEAR—have matured enough to devote resources towards higher-level analysis of their regional data. Performing link analysis and adding in

Table 3-4 Major ISS Query Types and Descriptions

Query Category	Query Description	Example Data Fields
People	Names, associates, aliases, relatives	Last name, first name, middle name, relationship, moniker
Locations	Address history, property history	Street, city, zip code, plate number, registration, owner history
Vehicles	Serial numbers, registration, make	VIN, plate number, model number

Table 3-5 Sample ISS Query Types

Query Type	CRIMES	CLEAR	FACTS	FINDER	INSITE	ARJIS
Last Name	✓	✓	✓	✓	✓	✓
First Name	✓	✓	✓	✓	✓	✓
Middle Name	✓	✓	✓	✓	✓	✓
Race (NCIC)	✓	✓		✓	✓	✓
Sex (NCIC)	✓	✓		✓	✓	✓
DOB	✓	✓	✓	✓	✓	✓
DOB Range (± 5 years)	✓	✓		✓		✓
Full Name	✓				✓	
SSN	✓	✓		✓	✓	✓
Status	✓	✓	✓			
Agency	✓	✓				✓
Warrants—links to	✓	✓				✓
Arrests—links to	✓	✓				✓
Field Interview Reports—links to	✓	✓				✓
State ID	✓	✓				✓
FBI ID	✓	✓			✓	
Operator's License Number	✓	✓				✓
License Plate	✓	✓	✓	✓	✓	
Vehicle Identification Number	✓	✓	✓	✓	✓	
Vehicle Year	✓	✓	✓	✓	✓	
Vehicle Make	✓	✓	✓	✓	✓	
Vehicle Model	✓	✓	✓	✓	✓	
Vehicle Activity Type	✓	✓	✓		✓	

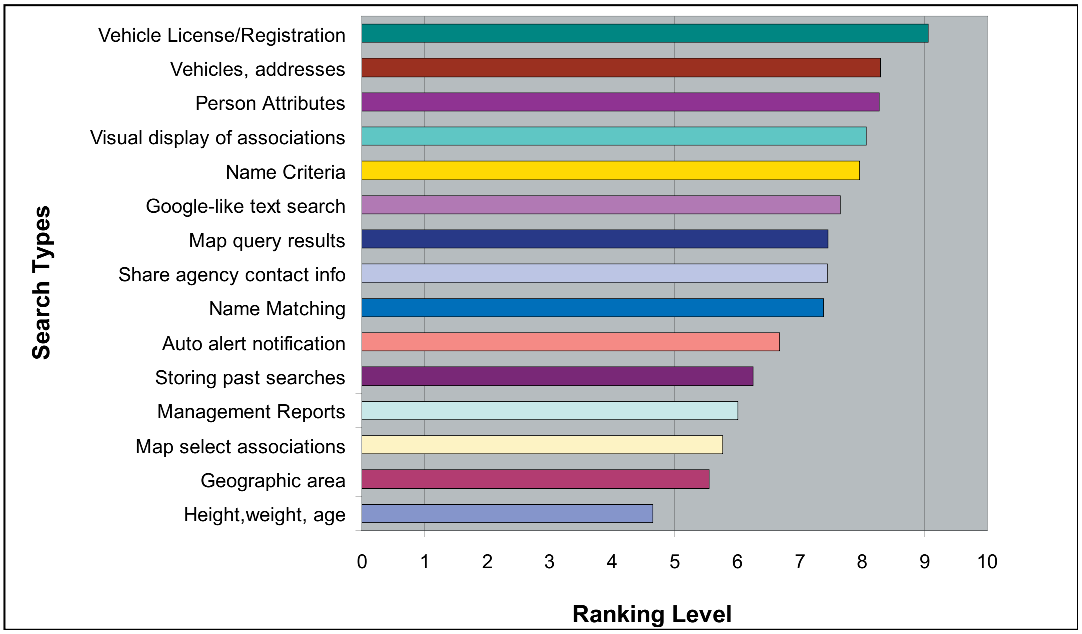


Figure 3-4 Ranking of Information Query Types Among ISS Participating Agencies

Table 3-6 ISS Analytical Capabilities Beyond Reporting

ISS Analytical Capabilities/Sources	ARJIS	CRIMES	CLEAR	FINDER	FACTS	INSITE
Crime mapping	✓		✓			
Officer safety alerts	✓	✓	✓			
Analysis tools (COPLink, I2, etc.)	✓		✓		✓	✓
Sex offender information	✓		✓	✓	✓	✓
Public data (Autotrack, Choicepoint)					✓	✓

automated rule sets or heuristics are now functions crime analysts need to sift through the ISS data. Investigators often use the results of an analysis for generating leads to solve related cases and to tie activities to the same subject.

The last item in Table 3-6—the use of public data sources by law enforcement—has been controversial. Analyzing public data sources for information on known criminals can only be done under probable-cause guidelines. ISS representatives related that the main privacy advocate issue was an objection to easier and faster access to—and searching of—public record data. Privacy advocates were concerned that the use of such enhanced capabilities could result in a higher probability of misuse of public record data by law enforcement. Privacy advocates claim that reducing the time and labor associated with correlating and searching public data threatens individual rights. Such past challenges must considered by any ISS organization. While the public data sources provide a wealth of analysis links for law enforcement, public perception and critics hamper adoption of public data sources by ISS organizations.

Unlike the more mature ARJIS and CLEAR ISS organizations, newer ISS organizations—such as CRIMES and FINDER—have a longer list of desired analysis capabilities, as seen in Table 3-7. Single sign-on is an issue expressed by a few organizations as a desired capability that would ease user access to information. Officers currently need to remember multiple passwords and respond to authentication questions multiple times. While some organizations like ARJIS have attempted to solve this issue through mechanisms such as a global query interface that provides a single access point to multiple data sources, other organizations face the complex task of balancing security requirements with the ease-of-use demanded by users for system access. Unlike the advanced link analysis functions offered by vendor products, the surveyed ISS organizations also indicated the need for more basic ways to link information in an automated fashion. Many agencies lacked the expertise and resources to send officers for training on interpreting, assembling, and effectively using the spider web link displays and tools typically characterized in vendor analysis software packages.

Table 3-7 Desired ISS Analytical Capabilities

Desired Capabilities	ARJIS	CRIMES	CLEAR	FINDER	FACTS	INSITE
Addition of digital files		✓		✓	✓	
Crime trending, bulletins				✓		
Crime mapping		✓		✓	✓	
Single sign on	✓			✓		
Access to criminal history records				✓		
Automated linking of information	✓	✓		✓	✓	✓
Single data entry	✓		✓			
CAD data		✓				
Deconfliction	✓	✓				

3.3.3 Structured and Unstructured Law Enforcement Data Sources

A typical law enforcement agency gathers information via many mechanisms that include both automated and manual processes. Command staff often acknowledge that a wealth of information exists in their agency but become frustrated in finding and correlating key bits in a timely fashion. This law enforcement data falls into two major categories: structured and unstructured. Table 3-8 lists examples of structured and unstructured law enforcement data sources. All the interviewed ISS organizations have unstructured data in all of these data sources.

Table 3-8 Examples of Structured and Unstructured Data Sources

Structured Data Source Types	Unstructured Data Sources
Records management database	Field interview cards
CAD database	Email messages
Accounting system	Voice mail
Payroll program	Fax messages
Personnel database	PowerPoint presentations

Structured data is mainly found in databases where every piece of information has an assigned format. The database clearly defines the fields, relationships, and attributes of the data. This organized repository allows users to run queries and formulas that extract useful, related information. Unlike manual processes, automated systems handle massive amounts of structured data quickly and efficiently. Table 3-9 shows examples of structured data sources from the surveyed ISS organizations.

Unstructured data comes in various forms that also may originate from automated and manual processes. Unstructured data does not have the same format, ease of search tools, and complex relationships found in structured data. Some types of unstructured data have some structural components, such as an email message's address header, subject line, and message body. Combined with attachments and typical storage of email message bodies in blobs rather than fields, email still falls under the unstructured classification. Paper archives, notes, and forms typically require an officer to sort and associate the information contained in them. Even in agencies with access to an ISS, there are still knowledge stores in unstructured data formats such as paper reports. Table 3-10 shows examples of the unstructured data sources from the surveyed ISS organizations.

Table 3-9 Examples of ISS Structure Data from Surveyed Sites

Structured Data Sources	ARJIS	CRIMES	CLEAR	FINDER	FACTS	INSITE
Records management system	✓	✓	✓	✓	✓	
Gang/intelligence data			✓			✓
Arrest information	✓	✓	✓	✓	✓	
Juvenile data	✓	✓	✓			

Table 3-10 Examples of ISS Unstructured Data from Surveyed Sites

Unstructured Data Sources	ARJIS	CRIMES	CLEAR	FINDER	FACTS	INSITE
Photos: mug shots, DMV, evidence		✓		✓	✓	
Agency employment application				✓	✓	
Field interviews	✓					
Paper-based warrants	✓			✓		
Local warrants in ISS database				✓		

3.3.4 User Interface and Functional Design Approach

Except for the client-server–based FACTS ISS, the surveyed ISS organizations all have a web-based user interface that incorporates many similar functions and features. Many law enforcement agencies are heavily invested in the Microsoft Windows desktop platform, which causes most users to expect a user interface that functions like a Microsoft-based operating system. Most ISS organizations simply replicated the basic Windows functions, menu styles, and navigation design through either the use of Microsoft development tools or third-party software packages. The interviewed agencies mentioned following one or more of the user interface and function design elements in Table 3-11.

3.4 ISS Operational System Descriptions and Best Practices

This section discusses the different types of ISS technical architectures and operational best practices, as well as how ISS organizations safeguard shared law enforcement information.

3.4.1 ISS Architecture Alternatives

A key component of any information-sharing program is the technical information system architecture that provides the infrastructure for exchanging and accessing data. While many custom variations and designs exist, the interviewed information-sharing programs have tended to use a distributed, centralized, or hybrid approach for sharing law enforcement information.

Table 3-11 User Interface and Functional Design Features

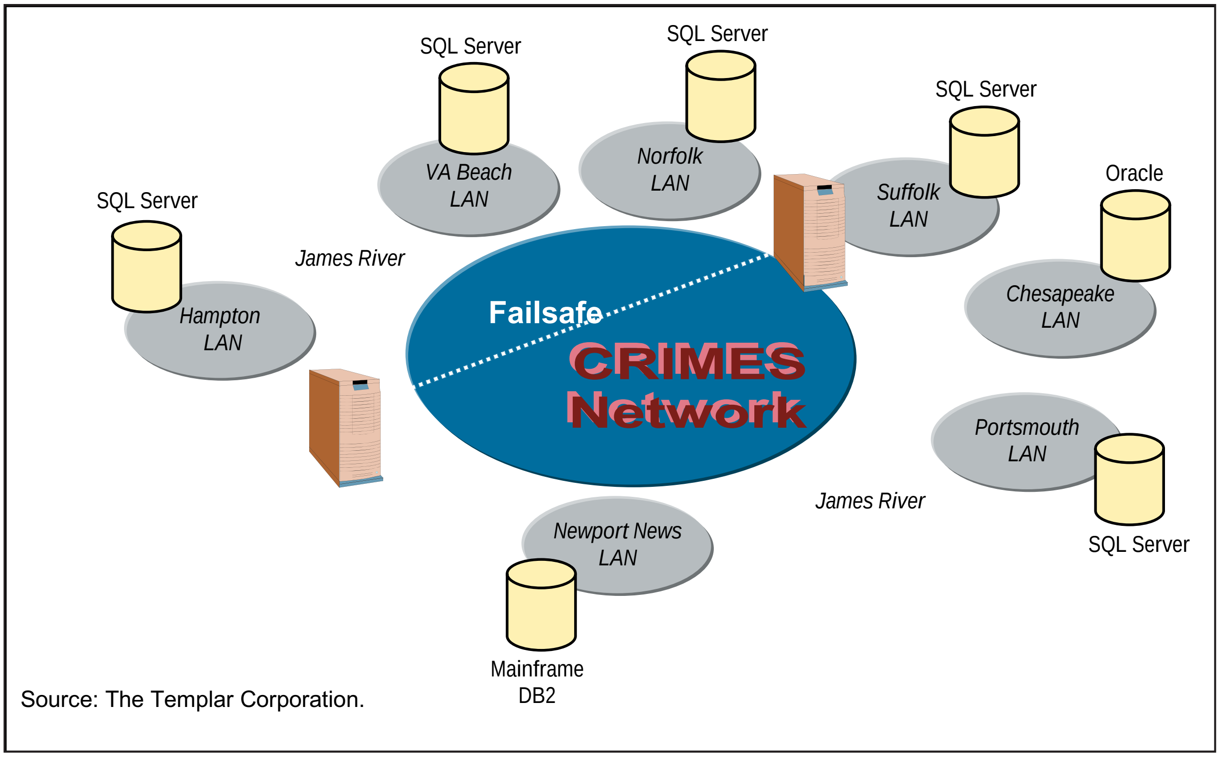
Features	ARJIS	CRIMES	CLEAR	FINDER	FACTS	INSITE
Data entered only once		✓	✓		✓	✓
Lists for related items	✓	✓	✓	✓	✓	✓
Use of structured query language	✓	✓	✓	✓	✓	✓
Informative error messages	✓			✓	✓	
Alarm definition by users	✓	✓	✓		✓	
User system status information			✓	✓		✓
Data field validation	✓		✓			

More mature ISSs tend to incorporate more guidelines than ISSs that have been created recently. Most of the user interface and functional design sessions were conducted with practitioner input from a variety of levels. All of the ISSs employ structured query language (SQL) for searching through data structures. A few system interfaces provide users with feedback about system update notifications and alerts based on user-set parameters. Although some systems—such as CLEAR—attempt to limit the amount of repeated data entry steps, many detectives and officers still complain about having to use multiple system interfaces and search methods to locate information. This problem is related to the desire for a single sign-on mechanism that would eliminate the need to remember multiple user names and passwords. While current efforts are under way to meet these needs and functional design requests, the technology may not be available or affordable to law enforcement agencies.

Each approach has advantages and disadvantages that may or may not map well into a region’s political, legal, and financial environment. The following sections discuss each architecture in greater detail.

3.4.1.1 Distributed Architecture

The distributed approach is an architecture alternative that is used by CRIMES, ARJIS, and FINDER. 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. As seen in Figure 3-5, each agency may have a different database product and may also have a different local RMS. FINDER and CRIMES agencies have interfaces that perform the communications linkage



Source: The Templar Corporation.

Figure 3-5 CRIMES Distributed Architecture

between the database and the main query server. While several technology-specific approaches exist for implementing the distributed architecture, such as Microsoft.Net and J2EE, the mechanisms and end goals are the same.

The distributed model offers several advantages to the ISS member agencies. This approach allows the ISS to avoid certain issues, such as managing a large, centralized data repository and the necessity of keeping a copy of agency data outside of agency-controlled facilities. Data ownership, access control, and any local ordinances would still apply at the agency level. The distributed data sources also allow ISS users to continue receiving data from the ISS even if a few agencies experience technical difficulties that have an adverse impact on data extraction.

Distributed architectures have grown over time as IT organizations have attempted to integrate information from different units of the same organization using the technology available at that time. This architecture suffers from a number of problems, which grow exponentially when inserted into a heterogeneous hardware and software environment. While it is initially appealing, the main problems (scalability and maintainability) end up being very costly even for small implementations.

Even though the distributed model offers some attractive benefits, there are issues with using this approach. Due to its distributed nature, this approach forces users to wait for responses from multiple sources that may respond within different timeframes. With CRIMES, data sources respond at different intervals or not at all depending on the number of requests on an agency database or whether the database is on line. Along with the longer search period, the distributed approach may require that each agency develop a custom interface to the ISS or extract and convert data into a common format and store it in a separate server within the agency's facility. As more agencies join the distributed model, the increased system complexity, administrative overhead, and system interface development requirements push the preference to migrate toward centralization. A larger amount of member agencies in a distributed model may also limit the development of the ISS community by possibly making it more difficult for local governments to agree on ISS operations and data sharing policies. The distributed approach makes building associations among data elements difficult due to the number of separate data sources the system must check. De-confliction is also not a typical feature of distributed systems as multiple records on the same suspect may exist in different jurisdictions for different offenses as each data source is independently managed.

Representatives from CRIMES, FINDER, and ARJIS all mentioned that creating the interfaces or extraction, translation, and loading (ETL) mechanisms is the most expensive part of linking new agencies into an ISS. As in the cases of FINDER and CRIMES, the distributed systems approach requires a programmer to write interfaces from each application to every other application with which it shares data. This approach results in enormous complexes of intricate, expensive, and redundant interfaces. Creating custom interfaces may also involve an in-depth understanding of the data exchanges, database structures, and query interfaces. Therefore, any ISS change may require each agency to change their interface. Comparing ISS organizations on this or any cost element is not possible since the financial costs vary in different development environments. FINDER uses University of Central Florida graduate students to program the ETL interfaces, whereas CRIMES uses a commercial vendor that charges industry-set software development labor rates. ARJIS combines the use of university graduate students with commercial contractors to meet their development needs.

Communication is also a key element in a distributed architecture. The distributed architecture relies on the communication link's bandwidth, speed, and reliability between sites to deliver information back and forth in a timely fashion. Compared to other architectures, the communication link dependency generates more "chatter" across the communication lines for distributed systems as end-user workstations must check data sources to query for information. A familiar distributed example is the National Law Enforcement Telecommunications System (NLETS), which links together states, federal programs, and justice-related programs.

Based on the national survey data, Figure 3-6 illustrates that a majority of law enforcement agencies rely on their local government internal networks to access law enforcement data. Almost half of the surveyed agencies have some wireless capability, though that includes both cellular technology and high-speed 802.11 data connections. The small number of agencies using leased lines reflects how few agencies have the budget to maintain commercial data services.

Figure 3-7 provides more detail on the type of communication bandwidth that agencies use to send data to vehicles and officers in the field. Low-bandwidth connections are still the predominant method for communications between vehicles and a dispatcher or station. Low-bandwidth connections typically consist of radio-frequency connections for voice and, in some cases, data transmission. Due to the cost and resources required to field a wireless system, less than 20 percent of the surveyed agencies have wi-fi connections to access data from the vehicles. Even fewer agencies have high-speed connections to handheld units, which may reflect again the cost of acquiring the equipment, supplying service, and performing maintenance. The

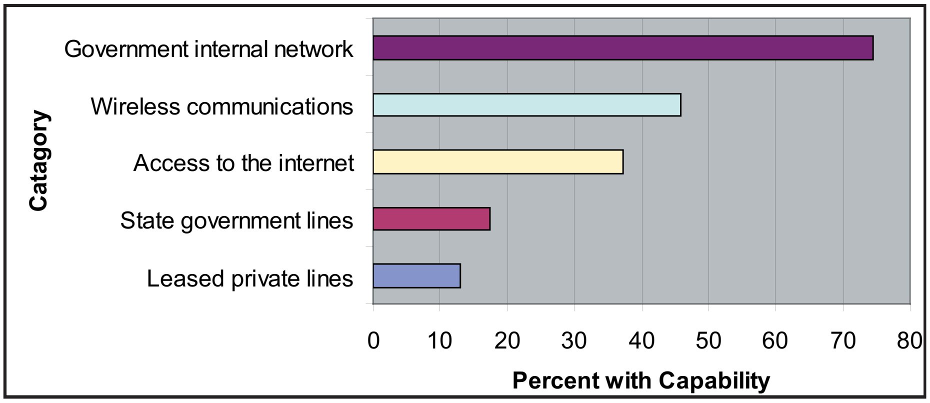


Figure 3-6 Agency System Communication Characteristics

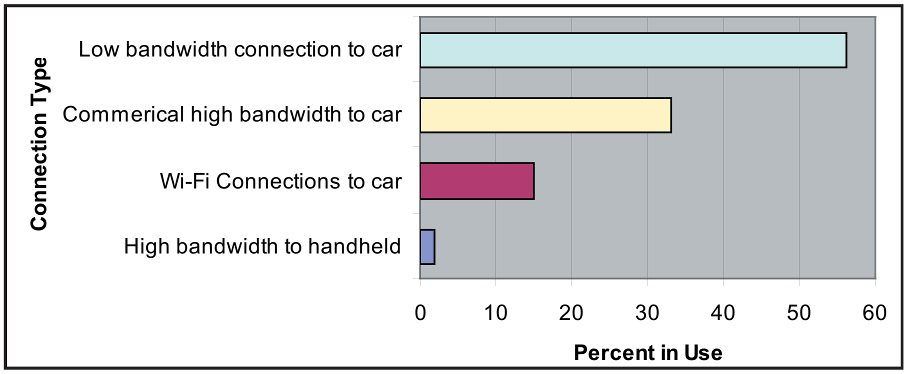


Figure 3-7 Communication Bandwidth to the Street

continued prevalence of low-bandwidth communication methods indicates that officers in the field may not have sufficient resources to directly access ISSs that send out large pieces of information, such as full rap sheets, multiple color photographs, and video files.

3.4.1.2 Centralized Architecture

The centralized architecture approach is used by FACTS and CLEAR (see Figure 3-8). This approach allows the ISS to have a main point of access and data management by dedicated staff in one main

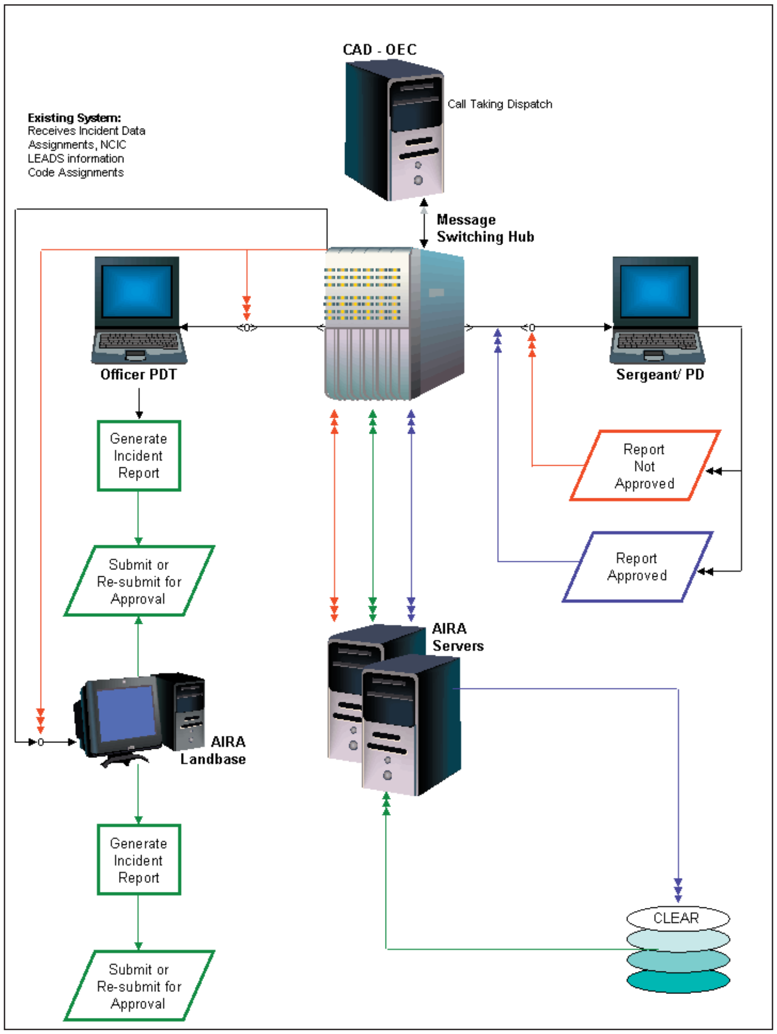


Figure 3-8 CLEAR Centralized ISS Architecture

location. The centralized approach typically involves a data warehouse that consists of records contributed by member agencies. Some ISS agencies, such as CLEAR and ARJIS, actually use the central database as their RMS. Each agency would access the central database for entering information and for researching case data. For CLEAR, the data warehouse provides the focal point for application logic changes and information analysis.

A number of benefits are associated with using the centralized architecture approach. Centralizing regional law enforcement data allows ISS users to start migrating toward a common understanding and terminology for the data they collect. Chicago's CLEAR system enjoys the benefits of "one-stop shopping" of information for officers interested in identifying a suspect. This approach allows an ISS to centralize analysis and reporting tools and allows applications—such as crime-mapping and link analysis—to readily draw upon a regional perspective of information from the central data repository. The central repository allows for a single point of data analysis to establish relations and associations. Systems such as CLEAR return results in a ranked order according to a set of heuristics for correlating search results. The system does not need to query multiple data sources that may report incomplete searches due to congested or underpowered network communication lines. A centralized system tends to incorporate more processing power and a homogeneous data structure. These two factors combine to reduce the complexity of integrating a data analysis tool into the ISS.

In spite of these benefits, there are a number of drawbacks to this architecture. While ISSs search multiple data sources on behalf of the users, the centralized approach raises several issues for ISS organizations. A failure or technical problem with the centralized data repository would take the ISS off line for all users. The centralized architecture raises the issue of who owns and manages the collated data and how data currency is maintained. The centralized data approach can also lead to misunderstandings about the use of a centralized database with privacy advocates or other special interest groups. However, issues are more likely to arise when other data sources, such as commercial data sources, are also housed in the data warehouse or accessed separately and combined with results from the centralized law enforcement database. NCIC is a well-recognized example of a centralized architecture as states transmit crime information to a central location managed by the FBI.

Although a centralized system might be the most cost-effective solution in the long-term because it uses a unified IT staff, this architecture may not be a feasible alternative for establishing an ISS because of political and technical issues. Creating a centralized system may require extensive data conversion and consolidation that may be too expensive for an ISS. An appropriate data center that has the proper environmental controls may not be available for hosting a centralized system. Although each agency typically decides what data to make available, a consolidated system would require each of those agencies to submit data that is then under the control of another entity. Additionally, the political and policy infrastructures that are in place make the establishment of centralized system architecture challenging to achieve. With the amount of time, effort, and funding already invested in each agency's operational systems, a centralized system approach could encounter tremendous resistance from the participating law enforcement agencies.

3.4.1.3 Hybrid Architecture: Combined Distributed and Centralized Components

After operating for several years, some ISS organizations—such as ARJIS—have capitalized on the benefits from combining the advantages of the distributed and centralized architectures. The hybrid architecture approach, shown in Figure 3-9, is more complex than either the centralized or distributed models since all issues from both approaches are combined. ARJIS program officials consider a successful ISS as having a combination of distributed, centralized, and federated elements. The term "federated" refers to how an ISS architecture consists of a system of systems where officers use a single interface to access several data sources hosted by different agencies that are distributed across an area. As ISS organizations grow and expand to include other agencies, the initial system architecture must be able to support the additional data and users. A hybrid approach provides the ability 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.

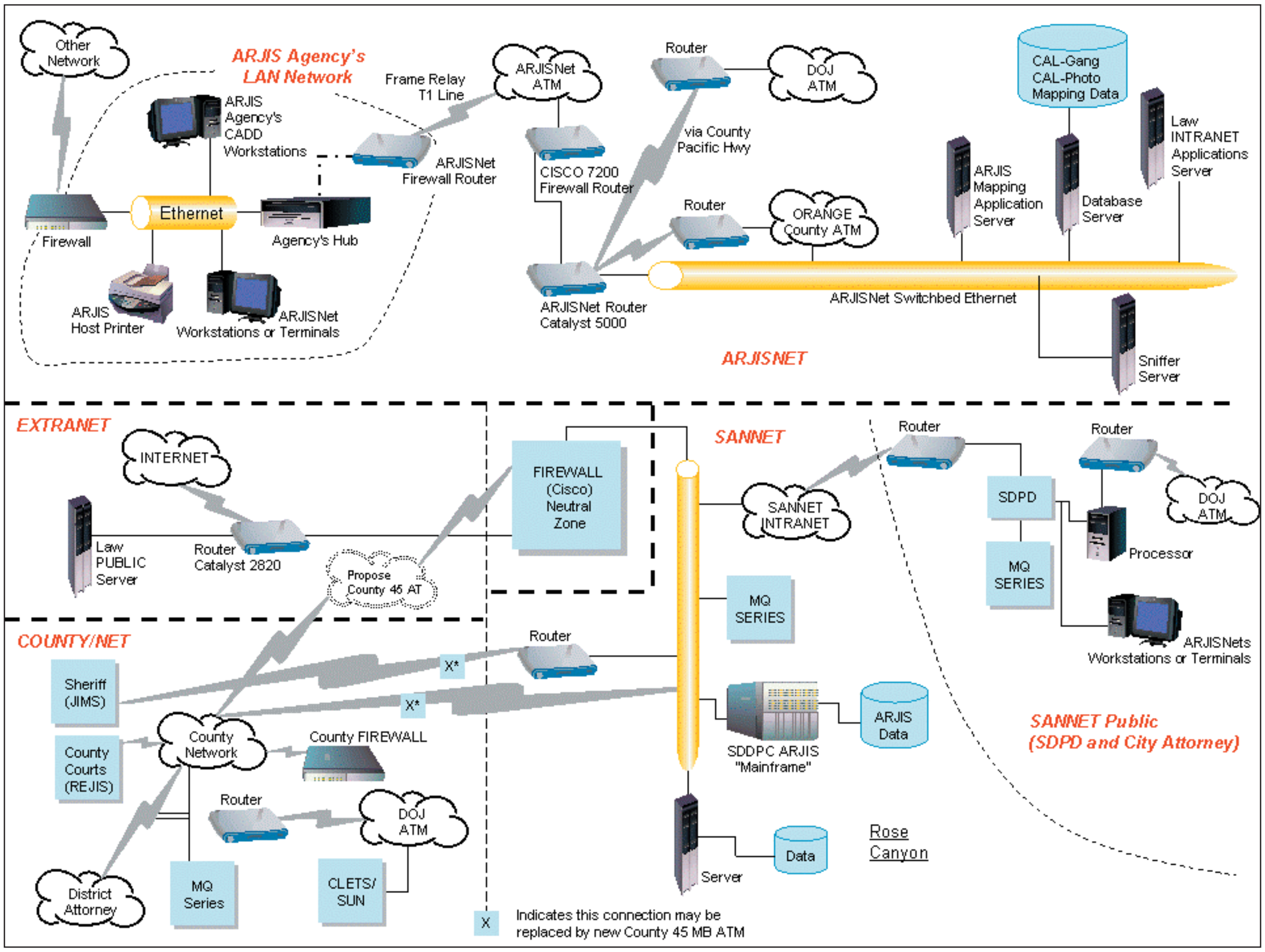


Figure 3-9 ARJIS Architecture

ARJIS has centralized databases in their mainframe and in databases on separate data warehouse servers. ARJIS also accesses distributed data sources, including systems at the state jail and Department of Motor Vehicles.

3.4.1.4 Architecture Feature Summary

Depending on the political, financial, and technological environment, one ISS architecture type may meet a region's needs better than another. The ISS organizations continue to evolve, which makes a strict comparison impossible. Regions interested in creating an ISS need to understand their local environment with respect to political, financial, and technological factors. Combined with a needs assessment, a region could then see which ISS in this document most resembles the functions, operation, and complexity that will meet their needs.

The more mature ISS organizations—such as ARJIS and CLEAR—have many features that other systems are just developing. Even within an architecture feature area, variations exist on how the implementation and design occurred. For example, ARJIS has a centralized database component but also includes a number of federated data sources and distributed users. Table 3-12 provides a list of regional characteristics and how they map against the centralized, distributed, and hybrid architectures.

3.4.2 ISS Architecture Best Practice Guidelines

Although the technical architecture approaches have fundamental differences, many of the surveyed ISS organizations share similar architecture features (shown in Table 3-13) that can be considered best practices. These features focus on higher-level technology concepts instead of the rapidly changing vendor landscape

Table 3-12 Regional Characteristic versus ISS Architecture Type

Regional Characteristic	Centralized	Distributed	Hybrid
Legal requirement to store data first in jurisdiction	✓	✓	✓
Dense population in large metropolitan areas	✓		✓
Rural areas or large unpopulated regions		✓	
Adjacent agencies with same RMS/CAD/other system	✓		✓
Outdated/low speed communications infrastructure		✓	
Legally cannot replicate data outside jurisdiction		✓	✓
Mixture of legacy systems created by multiple vendors		✓	
Few technical resources and people available	✓	✓	
Existing legacy sharing system	✓		✓

Table 3-13 Summary of ISS Architecture Features

Unstructured Data Sources	ARJIS	CLEAR	CRIMES	FINDER	FACTS	INSITE
Requires customized ETL interface	✓		✓	✓		
Uses centralized database components in ISS core architecture	✓	✓	✓		✓	✓
Contains GJXML interface	✓	✓		✓		
Demands high speed, large bandwidth	✓	✓		✓	✓	
Conducted privacy impact assessment	✓	✓			✓	✓
Ease of adding data analysis tools	✓	✓			✓	✓
Agencies perform local data updates	✓		✓	✓	✓	
Provides formal user feedback function		✓		✓	✓	
Centralized data sources	✓	✓				✓
Distributed data sources			✓	✓	✓	
Centralized operations management	✓	✓				✓
Distributed operations management			✓	✓	✓	
Hybrid operations and data sources	✓				✓	
Single point of access to all data sources		✓				✓
Federated search of agency sources	✓	✓		✓		✓

of products and functions. A new ISS organization or an existing organization interested in revising their technical architecture should consider the following set of best practices:

Thorough Testing and Evaluation: While a new technology may seem promising, allowing a technology to mature and conducting a pilot test are essential before adoption. Most of the ISS organizations have separate testing, development, and production environments for this purpose.

Standard Configuration Requirements: From CRIMES to CLEAR, all ISS organizations repeated the need for a standardized platform for the end-user client system. Installing updates to client machines on a timely and convenient schedule is a critical capability for maximizing ISS access for end users. ISS representatives indicated that the lowest amount of configuration on the end-client platform was a key factor in making the system scalable and manageable. Continuity of Operations and Disaster Recovery Plans: CLEAR and ARJIS, as well as other ISS organizations, recognize the need for such plans; both ISSs have experienced major system problems when servers and applications were not accessible to users. The Continuity of Operations Plan indicates the level of service and functionality that the ISS will continue to supply to users based on the extent of the system failure. The Disaster Recovery Plan focuses on the emergency contacts, system recovery steps, and data backup procedures.

Scheduled Technology/System Assessments: All of the ISSs realized that their systems need constant evaluation and fine-tuning to keep the systems useful to the end users. Although few had an official Capital Planning document, the governing ISS individuals recognized the importance of staying current with technology while looking for new ways to improve data accuracy and system efficiency while minimizing the labor resources required to maintain the system. ARJIS has learned that extra staff resources may be needed when fielding a new capability; they add extra computing resources so that the system can handle the large number of users that will attempt to try out the new capability. Once the new capability has been in use for a while, some of the extra resources can be redeployed for other purposes.

3.4.3 ISS Security Best Practice Guidelines

All of the ISS organizations recognized the need for secure communications and data storage. Many of the web-browser–based systems have security mechanisms in place to guard the transmission and submission of sensitive law enforcement data from the servers to the client machines. A hierarchical rule set typically governs who can access resources via different methods, such as remote access versus terminal access. CLEAR requires CPD users and partner law enforcement agencies to sign a security agreement prior to receiving access to the ISS. The following are considered a set of best practices for ensuring system security:

- **Use of Secure Socket Layer (SSL):** Several of the surveyed ISS systems use certificates for establishing SSL-encrypted connections from browsers back to the web servers. SSL is a common method for securing web-based applications while minimizing the need for constant client updates and complex key management systems.
- **Use Virtual Private Network (VPN) Links between ISS Member Agencies:** Federal law enforcement agencies have long used VPNs to secure their nationwide information systems. The ISS organizations recognized the need to secure their data communication channels while avoiding the expense of dedicated high-speed lines. Following the best practice set forth by the federal agencies, the interviewed ISS organizations also employed VPNs to link their member agencies.
- **User Account Control and Password Policy:** CRIMES and CLEAR employ user account controls that incorporate a password policy. Users who do not use the system after a finite amount of time have their accounts locked by the system. Administrators then contact the users to determine the reason for the inactivity. ISS organizations commonly use user IDs to audit and track user activity. These policies correspond to critical parts of computer security practices set forth by the U.S. General Accounting Office.
- **Auditing Requirements:** Most of the ISS personnel interviewed recommended implementing an auditing capability that allows system administrators to track changes to data files and other activities. Systems such as CRIMES had planned an internal auditing function but lacked the time and resources to develop the component. The auditing function provides management controls to ensure that the data is used for law enforcement purposes only and also illustrates the search patterns of users on the system.

3.4.4 User Training Best Practice Guidelines

Along with testing, training is typically the next underfunded and shortest phase of the SDLC. Software version updates, equipment updates, and end-user turnover all add to the difficulty of maintaining a core set of proficient users. Most of the emphasis remains on the system development and operational efforts, but training is an activity recognized by each of the interviewed ISS organizations.

Although user training times and material varied among the ISS organizations, three training approaches emerged from the interview results. Figure 3-10 shows the training approaches and the relative percentages of surveyed organizations using each respectively.

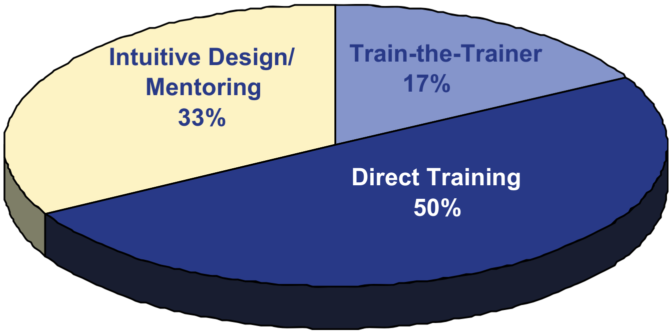


Figure 3-10 ISS Training Approaches

Three main training approaches are used by ISS organizations:

- **Train-the-Trainer:** ARJIS uses the train-the-trainer approach, which is commonly used in system development projects. 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.
- **Direct Training:** CPD and FDLE use direct training to provide officers with training in a classroom environment. The CPD incorporates CLEAR training as part of the police academy, while FDLE has full-time staff trainers to teach FACTS and InSite. The direct training method reaches the greatest number of users with the most consistent presentation of the ISS application.
- **Intuitive Design/Mentoring:** FINDER and CRIMES both indicated that their system interfaces have such intuitive designs that no formal training was necessary. Users have a set number of functions that searched specific types of information. As FINDER begins including more advanced functionality, the Consortium and the University of Central Florida recognize that they will need to schedule some training sessions.

Interviews of the six ISS organizations revealed that there are still problems with regard to training and information retention for personnel using the system. Many of the initial lessons and training are not used immediately even for younger officers who are accustomed to using computers. While many of the ISS organizations post a user's guide online that users can access, understanding how to create advanced reports or methods for querying information can be difficult for non-technical users.

While each approach has benefits and issues, a combination of elements from the three approaches would yield optimal results. CLEAR users receive the police academy training, refresher courses, and the benefits of uniformed advocates in each region. While the CLEAR interface may also be intuitive, training goes beyond performing simple searches and interpreting formatted results. Users must learn effective methods for developing queries that return information from various angles. Training users on how to exploit the system to answer their questions requires learning the thought process of using keywords, making associations, and detecting abnormal patterns. With more advanced analytical tools coming online in many of the surveyed regions, training will become even more important to detectives and other ISS users.

This page intentionally left blank

4 Issues and Impacts of Creating an ISS

This section discusses recommendations and lessons learned from the information-sharing programs. Although the interviewed representatives have ISSs that have been operational, each organization recognizes the need for improvement. Proactive approaches for minimizing the challenges associated with developing an ISS are also addressed.

4.1 Operational and Organizational Considerations

The six information-sharing programs interviewed have weathered many operational and organizational issues. The current officials in each program have recommendations and lessons learned for other agencies interested in implementing an ISS for sharing regional law enforcement information.

4.1.1 Governance

Establishing an information-sharing program will require a dedicated governance structure for management and oversight and a methodology for tracking progress. A short discussion on the governance process is provided first.

Law enforcement objectives and business goals drive the processes and operations that address the needs of the public. An information-sharing program will involve considering the traditional law enforcement goals on a regional level. The recommended architecture will change some of the current processes and operations to accommodate the shift to sharing information on a regional scale. The governance entity may need to examine how such changes in operations affect their performance in deterring crime and resolving incidents. One example would be implementing centralized dispatching. The mutual aid committee may monitor the new centralized dispatching operation and compare the performance to the previous decentralized approach. The performance results from consolidating dispatch may be so effective that other functions could then be centralized on that experience. The governance body would assess how best to apply the limited resources against business processes to meet the law enforcement objectives, as shown in Figure 4-1.

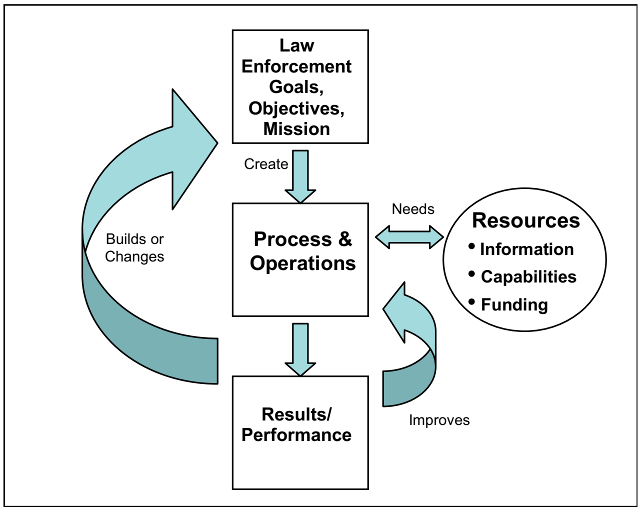


Figure 4-1 Governance Process

4.1.1.1 Governance Structure

The governance structure most commonly observed through the site interviews requires a strong foundation of representatives from the stakeholders. The ISS management staff should be limited, allowing the resources to be used toward operating expenses. As depicted in Figure 4-2, an appropriately sized structure for an information-sharing program would have a Director of Operations who is selected and supervised by a Board of Directors, which is made up of representatives from the member agencies. The Director would supervise the team of Communications and Network/ System Technicians that operate the ISS on a daily basis. The Board of Directors should be designed in such a way that various committees would address specific issues and report back to the body as a whole for final decisions. Advisory boards may be needed to help the Board keep abreast of the fast-paced changes that are endemic in the IT industry. Each of these governance entities is discussed in greater detail below.

Board of Directors. The Board of Directors should be made up of the Chiefs of Police of the member jurisdictions, elected officials, or a command staff member assigned by the chiefs. Political, economic, and technological realities suggest that the Board also contain a representative from other interested or potentially impacted regional agencies.

As an entity, the Board will be responsible for the following:

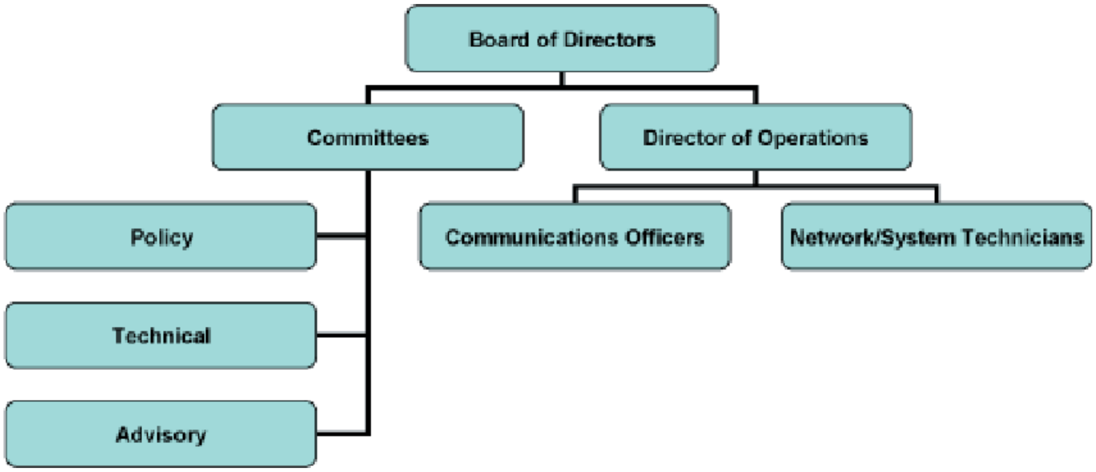


Figure 4-2 Governance Structure

- Developing the information-sharing program from concept to operational reality, including system planning through implementation
- Managing the overall program, including its personnel, operations, structure, and equipment
- Preparing and executing an appropriate MOU delineating cooperation and allowing for multi-jurisdictional operation of the center. The MOU may include the following specifics:
  - Authority to enter into agreement
  - Initial participants and participation levels
  - Resources contributed at outset
  - Resources to be contributed over time
  - How agencies are added or removed from ISS membership
  - Understanding and acceptance of the operational structure
  - How to determine operational needs and costs
  - How needs and costs would be divided among members
  - Initial staffing needs and source(s) of personnel
  - Description of data collected and from where
  - Description of data to be shared, among whom, and how
  - Responsibility to maintain infrastructure
- Enacting and maintaining Mutual Aid Agreements between agencies, if appropriate
- Equitably distributing information-sharing program resources among member agencies
- Ensuring that the ISS is in compliance with all applicable local, state, and federal laws
- Dedicating the resources necessary to create and maintain an effective information-sharing program
- Assessing and collecting fees from member agencies to support the information-sharing program's operation and development of future, expanded services
- Preparing and enforcing Standard Operating Procedures (SOPs) that will dictate proper ISS operations
- Creating and overseeing appropriate committees as may be required (see discussion below)
- Authorizing expenditures made on behalf of the information-sharing program
- Ensuring that the overall needs of the region primarily drive the ISS's service and technology decisions

4.1.2 Standing and Advisory Committees

In addition to sitting on the Board of Directors for the information-sharing program, each Board member will have many tasks within their given agency. Enacting the Standing and Advisory Committees recommended below will allow for the partitioning of some of the

Board's duties. The work of these committees can then be brought back to the entire Board for review, discussion, and voting. It is suggested that the Board of Directors create and monitor the activities of the following Standing Committees:

- **Business Process or Policy Committee.** The Business Process or Policy Committee would be responsible for the selection, acquisition, appropriate maintenance, and replacement of the ISS structure and non-technical physical equipment. The committee is also responsible for the ongoing adjustments to ISS policies as may be required from time to time, strategic planning, budgetary matters, and membership issues.
- **Technical Committee.** The Technical Committee would be responsible for the selection, acquisition, appropriate maintenance, and replacement of the ISS components. Further, the committee would be responsible for ensuring that adequate information security safeguards are in place and kept up to date, in both hardware and software forms, providing for data integrity and security needs. This committee is responsible for resolving any IT failures, keeping the Board updated on current technology trends and capabilities, system planning, and preparing an upgrade strategy as the ISS technology ages. It may be appropriate to subdivide the Technical Committee into Voice Communications, Hardware Systems, and Software Systems, depending on member's expertise. Decisions of the Technical Committee or any subcommittee would be ratified by the Board of Directors.

Additional standing committees may be formed and disbanded as the Board feels is appropriate in the execution of its duties. Any such committee should consist of representatives from the Board of Directors and other staff from member agencies.

Advisory committees should be established as necessary to conduct specialized assignments that occur on a periodic but irregular basis. Topics for these committees may include new membership application review, major system upgrades or overhauls, breach of security investigations, and malfeasance lawsuits. It may be prudent for the Board to enlist the help of professional consultants when dealing with certain highly technical matters or those dealing with potential/pending litigation. Membership of the advisory committees should include representatives from the Board of Directors, member agency staff, and topic specialists on an as-needed basis.

ARJIS is an example of a mature governance structure that embodies all of the discussed components. The Public Safety Policy Advisory Committee (PSPAC) of SANDAG is an organization that was formed to govern and operate ARJIS when ARJIS was consolidated with SANDAG. The PSPAC replaced the original ARJIS Board of Directors when ARJIS was consolidated with SANDAG. The PSPAC has a total of 15 members: 11 voting members and 4 non-voting members. The committee consists of 6 elected officials—mayors and council members (voting members) from four regions of San Diego County; 5 public safety members (voting members)—one county sheriff, one official from a regional homeland security department, one state public safety representative, and two representatives from the county chiefs/sheriffs association; and 4 public-safety advisory members (non-voting members)—two representatives from federal public safety agencies (U.S. Marshals Service, FBI, etc.), representative from the county (probation chief), and one representative from the courts system.

The PSPAC is the top tier of the governance structure that supports ARJIS. Below the PSPAC is the Chiefs'/Sheriff's Management Committee, which is supported by Advisory Committees that perform the business and technical work for the organization. Each committee formed has a committee charter that outlines its purpose, membership, and function.

Figure 4-3 illustrates the committees that have been formed for managing ARJIS. The Chiefs'/Sheriff's Management Committee primarily interfaces with the Business and Technical Committees, reviewing those committees' recommendations, which are then subject to approval by the PSPAC. The Business Committee determines the business needs for the entire region and develops the Business Plan, which recommends the types of projects to be implemented. The Technical Committee reviews the proposals from the Business Committee and evaluates them with respect to applying new technologies and standards. The Crime Analysis Committee evaluates and validates crime data and ensures DOJ and FBI reporting requirements

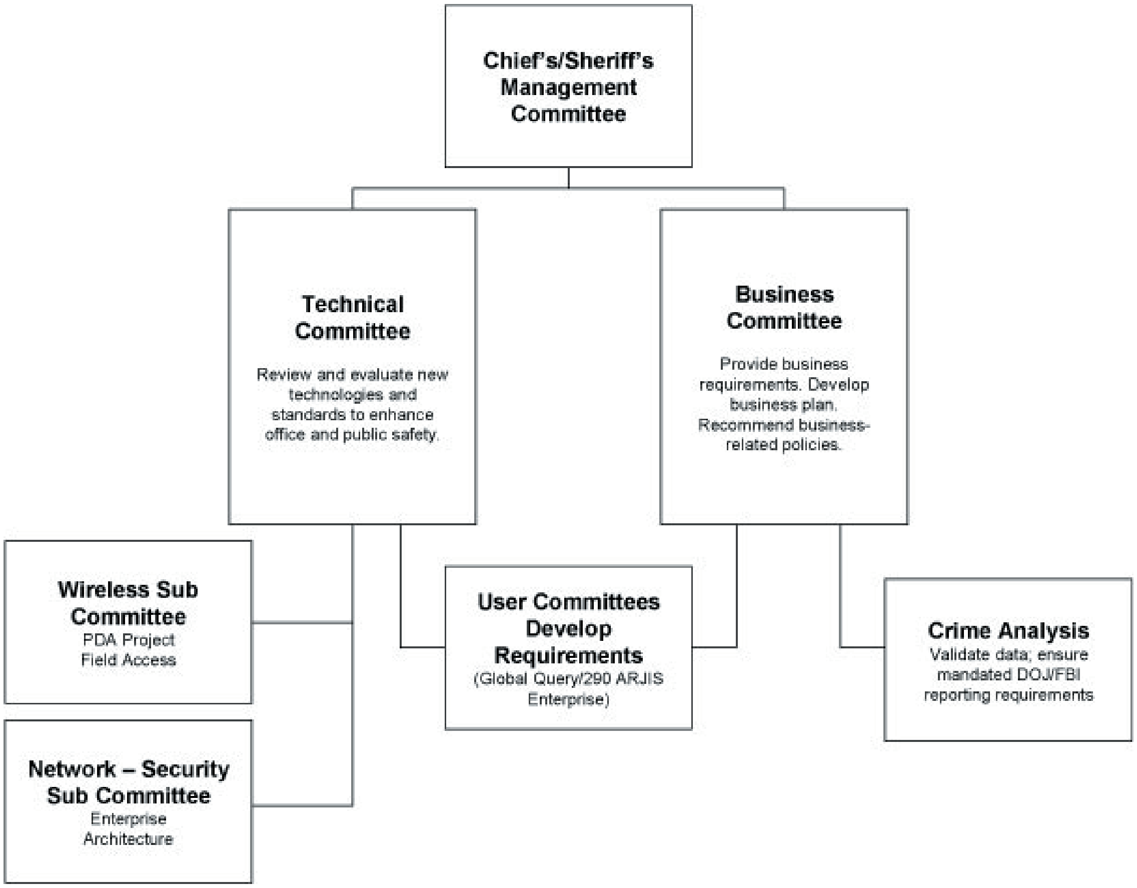

Chief's/Sheriff's Management Committee
Technical Committee
Review and evaluate new technologies and standards to enhance office and public safety.
Business Committee
Provide business requirements. Develop business plan. Recommend business-related policies.
Wireless Sub Committee
PDA Project Field Access
Network – Security Sub Committee
Enterprise Architecture
User Committees Develop Requirements
(Global Query/290 ARJIS Enterprise)
Crime Analysis
Validate data; ensure mandated DOJ/FBI reporting requirements

Figure 4-3 ARJIS Advisory Committee Structure[7]

are met; their assessment is provided to the Business Committee. The Wireless Sub-Committee was formed to assist with implementation of the Department of Homeland Security's BorderSafe Project, which is testing personal data assistants (PDAs) as a means of providing officers with wireless access to data. The sub-committee relays its results to the Technical Committee. The Network-Security Sub-Committee evaluates and makes recommendations on enterprise architecture; those results are also forwarded to the Technical Committee for review. The User Committees develop requirements for capabilities that directly affect users (e.g., for the Global Query) and sends its results to the Technical and Business Committees to be incorporated into their system enhancement recommendations.

The chiefs elect the committee members. Committee work is performed in addition to daily responsibilities. The objective of staffing the committees is to acquire a good balance of technical and business-oriented people participating with sworn officers in leadership roles. Chairpersons and vice chairpersons of the committees rotate every year; they are elected for two-year terms and can opt out of sitting as chair of a committee without any penalty when it is their turn. Currently, committees meet every month; however, there are recommendations to transition to meetings every other month. Minutes are captured at each meeting, including a list of attendees and actionable items, and are posted on the ARJIS web site. Chiefs are kept informed of all actionable items by the committee chairpersons who commonly are officers able to effectively communicate the business purpose of a proposed action. Staffing the Business Committee with personnel at the right managerial level to represent the agencies has been a challenge; ideally, committee members should include both uniformed officers and business-oriented individuals.

[7] *CRISP: ARJIS System Document* Appendix B, Reference 9

Although not all information-sharing programs interviewed feel that a formal governance structure is necessary, all of the surveyed ISSs do have a structured organization that coordinates ISS development, policy decisions, and program development. The governance structure is considered a critical factor for success by ARJIS and CRIMES. As CLEAR expands from the Chicago region to a statewide system (ICLEAR) it will transition from a system managed by CPD to one managed by a formal governance structure.

The CRIMES and FINDER systems are currently managed by strong governance boards with active participation from the member agency police chiefs. A strong governance board—in addition to one or more system advocates—is seen as a key factor in overcoming barriers to sharing information. Developing the CRIMES system required a single empowered project manager whose responsibilities were performed on a part-time basis. Recently, the CRIMES governance board has recognized that as more agencies come online, it will be necessary to fund a dedicated project manager position to meet the expected growth in managing the ISS cost-sharing plan.

4.1.3 Positive Impacts

Table 4-1 lists some of the positive impacts resulting from the use of an ISS, as described by the interviewees. The left column lists ISS objectives for agency staff that have direct use of the ISS. Objectives primarily relate to enhancing the effectiveness of personnel, which results from improved regional information-sharing. The right column provides one or more associated positive impacts that were reported.

4.1.4 Challenge Areas

As noted previously, use of a regional ISS provides a way to improve the operations of a participating agency. However, use of an ISS can also present challenges, as noted by the interviewed ISS personnel. Areas for improvement cited include the following:

- Data quality problems can jeopardize an officer's safety (e.g., warrant not displayed because agency data source is unavailable; warrant displayed when it should not have been due to erroneous data entry procedures by an agency).
- Information returned may be voluminous and unfiltered; too much data can conceal critical information the user desires.
- User interface screens are not tailored for each group of end users (for instance, the dispatcher may need to quickly locate information that may affect an officer's safety; the same query user interface that supports a detective's use of the system may not support the dispatcher or the dispatcher may require more training).
- The absence of a time- and cost-effective training approach can result in a lack of user training.
- The process for implementing change does not always include user community involvement, which can necessitate additional user retraining.
- There are times when the system is inaccessible:
  - Incompatible user hardware, software, or out-of-date configuration settings and other such considerations that are the responsibility of the individual agency's limited and often overburdened IT staff and funding resources
  - Lack of broadband wireless for patrol car access
- System may have inconsistent results/data currency problems (e.g., incomplete information when an agency data source is off-line for a period and no data can be retrieved from that database)
- There can be problems with data quality (e.g., inadequate regression testing resulting in problems after a new system baseline is placed into production, such as providing inconsistent or incomplete data responses to the same query)

4.2 Success Factors

The factors in these subsections present approaches in the following areas that contributed to the success of the ISS programs interviewed:

- Governance
- Operations
- System Design and Development
- System Functional Capabilities
- Training
- System Promotion
- System Procurement

Table 4-1 ISS End User Discussed Objectives and Positive Impacts

ISS Objective	Positive Impacts
Detective/Investigator	
Increased Case Closures	More detailed data on the suspect, narrative information detailing past incidents, and the ability to connect one person or objects with others contribute to successful case closures.
	The system has proved to be a viable tool for detectives to use in tracking down suspects and closing cases that they could not have completed using conventional techniques.
Improved Officer Safety (e.g., during arrests)	Additional data can protect the arresting officer by providing more detailed information regarding subject and addresses where subject may be apprehended. Officer safety during police raids is significantly enhanced by having all field personnel at the scene view videos of the target area on PDAs prior to the initiation of the raid.
Increased Suspect Leads	The system provides detectives and investigators with increased capabilities to generate leads, profile suspects, and locate stolen property that would not otherwise be possible.
Increased Detective Productivity	The Officer Notification System feature provides detectives with potential hits against INS warrants that have not been or might not be entered into NCIC. Hundreds of cases have benefited from more and better leads.
	The system makes it easy to identify and investigate possible suspects who have been convicted of smaller/lesser crimes of vandalism, theft since it is known that such activity frequently leads to higher profile crime and dangerous associates.
	The system's capability to recognize subjects previously arrested and paroled leads to more successful arrests. Searches can be conducted without the lengthy process of obtaining a warrant when the officer knows that the suspect's 4th Amendment rights are waived.
	Narrative in the incident reports provides detailed information that is not available in criminal-history reports (e.g., involvement in domestic violence).
Crime Analyst	
Improved Crime Prevention	System supports agency COMPSTAT process with impacts from the wider jurisdictional area.
Improved Officer Safety (e.g., during patrols)	System provides target patrols with more and detailed information on suspects and activities.
	The real-time processing capability of the mapping application, coupled with the accuracy of GEO-coded addresses, enhances officer safety when responding to calls in potentially dangerous areas.
Improved Crime Analyst Productivity	The productivity gained through the use of the mapping application to run searches involving sex offenders made it possible to reduce staff.
	Crime analysis tools are put directly into the hands of officers to enable early assessment of criminal activity and to provide more detailed information for the crime analyst to use in subsequent crime-pattern identifications.
	The system facilitates crime analyst reporting to the state level regarding information that is collected and shared regionally.

Table 4-1 ISS End User Discussed Objectives and Positive Impacts (concluded)

ISS Objective	Positive Impacts
	The system has a profound positive impact on customer service, criminal analysis profiling, and automated pawn data processing, all of which would suffer greatly or no longer be practical without it.
	The system enables easy access to modus operandi information that can be used in the mapping application to track particular types of criminal activities.
Intelligence Analyst	
Improved coordination of intelligence operations	Moving violations or other tickets can show that person is in a certain area.
Improved success of intelligence mission/case closures	Users can find and provide accurate information on where a drug suspect lives and works, names and dates of birth used, and criminal activities involved with the suspect.
Improved access to intelligence information	Narrative on incident reports can confirm type of drug associated with person.
	Information on vehicles used in drug-related incidents can be traced to source, such as single rental agency.
Patrol Officer	
Improved Officer Safety	The use of a PDA increases patrol officer safety by enabling access to system information or receipt of alerts about potential dangers at a location being investigated or those at the scene of a criminal activity.
	The PDA provides a patrol officer with an essential backup capability if there are CAD failures or if there is a priority event that ties up the main PD Radio Inquiry Channel.
	The PDA enables officers to access digital photos, which enhance the officers' ability to make positive identifications of potentially dangerous individuals.
Increased Productivity—More Time on Patrol	Patrol officers' access to ISS data via PDAs saves time since they do not need to access each member agency's data directly.
	The ability to use a voice-recording PDA enables officers to record events at a scene that could later be more efficiently entered into the officer's report.
	The system's speed, accuracy, and data availability enable officers in the field to run more suspect ID and vehicle license checks without impacting the functions of the dispatcher.

Source: June 2006, this table is based on information from the interviews sites.

4.2.1 Governance

Establishing a strong governance or management entity to oversee ISS development and establishing appropriate policies and procedures for use and operation of the ISS are extremely important to the implementation of a successful ISS program. It is essential to build a collaborative environment made up of individuals who can see beyond individual jurisdictional needs to the needs of the region and are willing to act proactively to work issues that can affect ISS success. In some ways, the strength of the governance or management body is reflected in the level of success of the ISS implemented. Individual factors cited that contribute to strong governance follow.

- A strong advocate is needed to initiate the project/system.
- Implementing a collaborative form of governance ensures successful ISS management.
- Legislative support for the system must be developed to establish long-term financial and

operational viability of the system. The support of a legislative body can better ensure continued funding for the program.

- Organizational bylaws need to be developed to establish a foundation for ISS governance.
- Law enforcement and ISS governance personnel must reach a common ground with respect to the existence of ISS bylaws that dictate system use and operation.
- Creating a business plan is instrumental in specifying the program's goals and how to achieve them. The effort to implement an ISS program should not go forward without a credible business plan.
- An MOU must be developed to sufficiently address each area for governing the ISS while remaining flexible, expandable, and adaptable to support the needs of the participating agencies as the governance process matures.
- Providing for one vote per agency with simple majority for passage creates a positive environment for members to raise issues and gain resolution in a fair manner without regard to agency size or agenda.
- The ability to manage budget and policy changes through flexible governance procedures can minimize recurring need for legal consultation.
- Periodically assessing the governance charter and its bylaws keeps them relevant to the members and the mission as changes occur.
- A security agreement should be defined and signed prior to sharing any data.
- Active participation by police chiefs on the Governance Board was critical for timely and informed decision-making to facilitate information-sharing across agency boundaries, which enabled the program to move forward.
- Requiring agencies to have appropriate personnel attend governance meetings ensures that meaningful communication takes place and results in actions that benefit all members.
- Stakeholders should believe in the program and support its establishment, sustenance, and membership.
- Individuals who will embrace the technology should be engaged even if they are not technologically astute but see it as a way to further the capabilities of the organization and even their careers.
- It is important to concentrate more on anticipating issues rather than revisiting lessons learned.
- The use of focus groups to work through complex issues and bring their recommendations to the membership results in more actionable proposals.
- The use of special task forces to spearhead system design and development is vital for success.
- A data-sharing policy should be implemented that does not assume all participants will share their data equally.
- Smaller agencies must not be overlooked as potential members of the ISS. Membership should be extended to other public-safety organizations (e.g., fire departments and prosecutor offices) that could benefit from access to criminal subject or activity information.

4.2.2 System Procurement

Many of the same issues that must be addressed when procuring an information system for a single agency also apply to procuring a regional ISS. Interviewed ISS personnel offered insight on what worked for them when they were going through the procurement process.

- ISS success can be attributed to its lack of dependence on a single vendor-based system solution.
- Vendors need to be thoroughly vetted to avoid pitfalls of employing vendor-specific solutions that become prematurely obsolete.
- Thoroughly assessing baseline requirements against available commercial off-the-shelf (COTS) products allows only viable products to be acquired.
- The best technical solution needs to be selected, whether it is vendor-based or requires an in-house staff effort, even if essential in-house skills are lacking.

- To avoid costly change requests, it is always desirable to negotiate for source code rights when procuring a vendor-based solution.
- Public safety member agencies need to be educated on vendor management techniques.
- It is vital to recognize that maintenance and vendor support cost agreements are key elements in any COTS product acquisition.
- Establishing a proof-of-concept prototype with a proposed vendor product prior to fully committing to it eliminates unnecessary technical and cost risk.

4.2.3 System Design and Development

ISS personnel interviewed considered one or more of the following factors important in designing and developing their regional system. These responses highlight the need to involve the right people and provide adequate time for planning and system design to ensure that the ISS will support regional needs.

- Business needs, expressed through use cases, define the requirements that drive build-or-buy decisions for new development capabilities.
- System development that is based on a bottoms-up, prioritized methodology makes future application development possible and practical.
- The development of the system should follow the project management life cycle with a well-defined project scope and schedule.
- The development should use an iterative approach, and implement a change control board to manage and approve changes to the system design.
- The effort expended in functional system design provides the most benefit when compared to amassing voluminous amounts of data too large to process.
- Local member agencies must actively participate in the development of the ISS by stating which system features are needed and how their agencies' data is handled.
- The ISS must provide a one-stop shopping capability for users to access requested data. This capability can also streamline work processes.
- By making the system user-friendly from the start, users are more likely to see the benefits that come from using it. Maintaining a consistent system graphical user interface (GUI) facilitates user acceptance and minimizes the need for refresher training.
- Building information-sharing applications that use web-based services and conform to GJXML standards is efficient, cost-effective, and more easily assimilated by users.
- Elimination of multiple applications, multiple databases, and multiple programming languages simplifies operational maintenance.
- Be prepared to deal with unforeseen or unknown recurring development costs due to project/system changes.
- Users accessing one system vs. multiple systems have to remember only a single username and password.
- Legacy software conversion (COBOL code) and technology upgrade (web interface) transition efforts are often more successful than a complete system functional redesign due to the familiarity that developers have with the existing design.
- The involvement of end users experienced in all of the system's functions is crucial to a successful transition.
- System development is successful when the right users—those with a stake in the success of the system—are involved in and committed to the development from the beginning.
- The input from end users in the application development and change processes is instrumental in producing effective solutions that users can more readily accept.
- Gaining agency consensus and adoption of core common user forms and input formats can establish a successful pattern for other agencies to follow.
- Internal IT skill sets can be leveraged throughout development of the system to minimize costs associated with the need for vendor involvement.

4.2.4 System Functional Capabilities

A number of features and capabilities were identified by ISSs that impacted users' desire to use the system. These include features that are optimized to support searching and analyzing large volumes of data, whether centrally stored or distributed. These capabilities increase the efficiency of participating agencies, which is an indication of ISS success.

- A method of recording successes realized through the use of the ISS needs to be incorporated.
- The ability to execute a saved query enables detectives to retrieve updated results for previously executed queries.
- Being able to identify "Who's at an address" is instrumental for locating/identifying multiple persons at an address.
- Business name/employee name search is extremely useful in showing associations among people at a business address or business phone number.
- Wildcard searches are extremely effective for pattern-matching operations.
- Single search capability of multiple data sources maximizes user efficiency.
- Multiple search parameter capability provides more complete result set.
- Comprehensive reports are critical for developing leads and can be a factor in efficiently closing cases.
- User interface is easy to use; application is intuitive and becomes irreplaceable.
- Generation of periodic reports is used to facilitate quality control.
- Link association between state data and public record data creates leads.
- The link association chart feature provides a superior visual aid in forward and backward link assessment.
- Record creation is more efficient through the use of the Automated Arrest program that was brought about with the implementation of the system.

4.2.5 Training

Realizing the benefits of providing sufficient training, and structuring training in ways that best promote initial and continued use of the ISS were also considered very important. A proper approach ensures that end users have a clear understanding of how the ISS is envisioned to be used and incorporated as part of daily operations. Interviewed ISS personnel reported the following success factors associated with training.

- To minimize the amount of training needed, the system was designed to be easy to use without extensive training and written documentation.
- A train-the-trainers approach—along with each agency being responsible for training its own users—is successful and cost-effective.
- System training introduces new capabilities/functions that give users a better appreciation of how the system can assist them in their tasks.
- Hands-on training with real-world cases facilitates users' acceptance of system tools.
- Officers are involved in developing the training regimen to define content relevant for fellow officers. In a similar theme, system training conducted by sworn officers for sworn officers is more effective than training by civilian staff.
- A positive training experience can result in trained personnel promoting the system to other officers, thereby increasing usage and providing mentoring support to new users.
- Privacy laws and information dissemination procedures (both internal and external) must be covered during training.
- Recorded success stories are effective training aids.
- Training is needed so that the ISS is used accurately to avoid invalid results.
- Training is easier, more effective and less time-consuming with a single system than with multiple systems.

4.2.6 Operations

Success factors that impacted the ISS after it became operational were also provided by those interviewed and are listed below. These factors address scalability of the ISS and other capabilities that were incorporated to ease system administration and maintenance.

- Agency personnel authorized access for their own end users and managed the secure communication and database access to their data source.
- Unlimited user licenses are needed to support all current and future users.
- Automated installer tools simplify user (client) installations.
- It is important to ensure that the system has high availability.
- Flexible work processes are required to enable adaptation of user-induced changes or technology advancements that are often associated with IT application development.
- System usage is audited to ensure that users abide by established rules and procedures.
- Skilled, part-time IT personnel can be efficiently employed for fixed-duration tasks, thereby allowing for a smaller, more economical operational staff.
- Member agencies with large IT staffs can be an excellent source of manpower.
- Gaining member agency agreement on law enforcement data-entry standards and procedures is key for enabling a regional search capability.
- Consistent and verifiable search results are facilitated by differentiating and categorizing input data accurately.
- The system scales to accommodate the addition of member agencies while maintaining operational performance levels.
- New system releases should be deployed during periods when users are likely to get needed support—not at the end of day or work week when the full complement of IT support staff are not in the office.

4.2.7 System Promotion

The need for formal activities to promote use of the ISS should not be overlooked. Promoting the system—both internally to participating agency users and externally to prospective member agencies—is seen as essential by interviewed ISS personnel.

- The system should be actively marketed to targeted groups and not be expected to sell itself.
- Agency system advocates should be identified and required to champion projects and market the system internally.
- The initial promotion and implementation of the ISS needs to be directed toward the most prevalent criminal-related activity (e.g., stolen property/pawning) in the region.
- System consistency and reliability helps promote user buy-in.
- Promoting the ISS is immeasurably benefited by individuals who have experience in law enforcement and system development.
- The ISS's promotion is greatly enhanced with the increase in the number of member agencies.
- A capability needs to be developed to demonstrate the functionality of the ISS before promoting the system.
- The ISS must first be promoted to the end users (e.g., investigators) who can most benefit from the system.
- Promotion of the system is more effective through active interaction with potential stakeholders.
- Maintaining a dialogue with the users via email and telephone support assists in establishing satisfied users.
- Sharing novel approaches to solving cases via success stories encourages others to use the system more effectively.
- Promoting the system requires awareness of the community's concerns with respect to criminal activity.
- System proponents should be open to the needs of other law enforcement agencies and external (federal/state) entities that could be the foundation for future system interfaces or integrated functionality.
- Agencies willing to share their law enforcement data with other agencies are more likely to receive such information in return.
- A key to promoting the system is involving sworn officers.

- The public relations function needs to favorably characterize the system both internally and externally to appropriate stakeholders.

4.3 Lessons Learned

In addition to the success factors identified in Section 4.2, interviewed ISS personnel also provided specific recommendations that were considered lessons learned during the course of establishing their ISS program and implementing their regional system. While some of these lessons learned were implemented by a few of the interviewed ISSs, most of these recommendations address approaches that were identified in retrospect. These recommendations are items that one or more ISSs realized they should have done or should do, but had not yet implemented by the time of the CRISP interviews.

4.3.1 Governance

ISSs provided a large number of lessons learned for governance; highlighting again the need to recognize that establishing and maintaining a strong governance and management structure is essential for a successful ISS program.

- In order to help establish sharing guidelines and expedite system agreement signatures, each agency should identify a single agency attorney to review the agreement for a city manager and city clerk to then approve.
- An Oversight Committee should be formed to address any violations of the guidelines established by the Executive Board of Directors.
- A Users Committee should guide the specification of requirements and user interface design to meet the needs of users rather than leaving such decisions to IT professionals.
- An Evaluation Committee is needed to investigate the system's effectiveness in meeting the needs of the agencies. This committee should define which metrics to capture and what analysis to use in processing those metrics.
- Contract management must be in place to have a vendor develop or support the ISS according to specifications.
- Agencies must manage ISS funding and develop funding sources for future capital and operating expenses; agencies should establish purchasing rules based on the different agency policies.
- Agencies should enact a policy making the use of the system mandatory.
- United leadership and a strong advocate are needed to stand up and sustain the program.
- Define an approach for dealing with antiquated policies and procedures that are not relevant to the program or the technology being deployed.
- Criminal intelligence information programs need to implement proper guidelines and procedures to ensure smooth system development and operations.
- Allow all stakeholders to access information whether or not they contribute data.
- Smaller agencies lacking resources (funds/equipment) should be supported to maximize the value of criminal intelligence information.
- States should share their criminal intelligence information by overcoming the constraints imposed by individual state regulations.
- Understand the restrictions that a state or agency places on the data it provides before accessing the data and potentially violating legislation on its use.
- The governance structure of the ISS should convince agencies to make an initial investment in the ISS (funds, resources, etc.) based on an expected return of investment.
- The governance structure should stipulate that agency participation entails contributing data to the system, as well as retrieving data from the system.
- The governance structure should convince government commissions and political leaders to support the adoption and implementation of the ISS.
- Logistical issues—such as coordinating meetings, telecons, and scheduling—in multi-participant systems can be time-consuming; a concerted effort should be made to accomplish these tasks as efficiently as possible.

- The governance structure should develop an ISS privacy plan to control information handling and dissemination.
- MOUs and other legal agreements should consider the need for multiple legal counsel-related inputs in decision-making.
- A privacy plan should be implemented that meets a standard appropriate to the project and system; include the criteria that privacy advocates are expecting.
- Review the Global Information-Sharing Plan (GISP) regarding recommendations on sharing systems.
- Review what other states are doing in information-sharing.
- In order for the system to grow as a regional system, it must enable law enforcement data entry from all potential members.
- Be aware of political, social, and other sensitive issues that could have a negative impact on moving the program forward.
- Leadership is required at the national level to develop law enforcement information-sharing privacy policies and information exchange standards.
- The key to effective governance is to gain the support of member agencies by establishing clear goals for information-sharing that can be fully embraced and accepted by the members.
- Dialogues should take place among law enforcement and legislative bodies to reach a consensus on regulations that apply to law enforcement information collection, storage, transmission, retention, and privacy requirements.
- ISSs should have an auditing capability to account for the use and dissemination of law enforcement data.
- Member agencies need to focus on sharing daily operations information (e.g., subject identification and prior criminal history) to maximize the program's effectiveness.

4.3.2 Procurement

A planned procurement should result in a vendor and product that better suits user needs. While procurement and source selection is often a difficult task, the following lessons learned should help new ISS organizations with some insight on how to broker better terms with vendors.

- Review what other states have done to implement information-sharing, and leverage that approach if appropriate.
- The ISS management should evaluate vendors to avoid rigid contractual agreements.
- The ISS management should negotiate for unlimited user licensing.
- Consider the possibility of changes in vendor relationship during the lifecycle of the project/system—for example, changes due to a vendor being taken over by a larger company, historical knowledge lost due to vendor's key staff working closely on your project leaving the company; unknown future costs due to contract renegotiations.
- A tight contractual vehicle with multi-year negotiated costs and provisions for enabling strong oversight is necessary to control requirements creep and schedule slippage.
- There is a need for a regional procurement strategy as more agencies join the information-sharing program to provide leveraging power with vendors and contractors.

4.3.3 Development

Any large system will require some amount of customization and tailoring to meet the needs of a diverse client base. Although the mission may be similar, regions interested in forming an ISS often have different formats of data, incompatible legacy systems, and variations in law enforcement business processes. The following lessons learned should help guide new organizations with developing an ISS that will be better suited for their needs.

- The largest and most difficult information-sharing IT task lies in mapping the existing legacy information to a new, standardized format.
- There is a tradeoff to be made in avoiding conversion of legacy information by maintaining

two operational system modes: one for legacy data and one for the new standardized format.

- Users are a critical component in the development process of the system because they contribute to the functional definition and provide feedback to the system developers.
- Enable police officers to contribute to the development process and gain a sense of system ownership as a result.
- Union regulations and management policy can affect the design and development process and should be addressed early.
- Mandate that the institutional knowledge gained by the development team and project management staff be retained through thorough documentation procedures.
- Reduce anxiety of the public by building a public version of the system.
- Be prepared to take risks, but implement a risk management plan to proactively assess potential problems and ways to mitigate them.
- Predefine data types to be used in the system to create a common format that would mitigate the need to enter data twice—once in a personal log and once in the RMS; enable more data to be shared.
- The ISS should be initially implemented among larger participating agencies to gather the critical mass of data that will enable practical use of the system.
- The ISS should adopt a set of development standards that facilitate data exchange among participating agencies.
- An automated ETL process should be developed to support scalability of the ISS.
- The ISS should be developed to meet IT industry standards (at a minimum).
- ISS development and maintenance plans should be devised to support continuity of the system in the absence of the original development team.
- System development needs to take into consideration potential significant technical issues related to transitioning from multiple operational systems into a consolidated system.

4.3.4 System Functional Design

Developing a system requires a combination of technical, business process, and human factor elements. Designing an ISS with the following lessons learned will help new ISS programs avoid the difficulties experienced by the veteran ISS organizations.

- The design involved a user group with participation from all users (analysts, dispatchers, etc.); user functionality should not be designed by technical staff (agency or vendor).
- System statistical reports should be uniform across all member agencies to allow for valid regional comparisons of system performance.
- The system's functional design should comply with standardized law enforcement information codes.
- Limiting types of data that can be stored in the data warehouse helps to use limited resources to provide adequate system response time.
- The gradual transition from a paper RMS to an electronic RMS promotes the new system's acceptance among law enforcement personnel and allows them to adapt to it more easily.
- The system design includes access to highly desirable mug shot data and is particularly useful within the crime mapping function, which can display photos of suspects, associates, and relatives.
- Deploy systems supporting daily law enforcement (crime-related) needs (FACTS) along with those for intelligence purposes (InSite) in such a way that all information is available to those individuals working on intelligence cases (InSite users).
- Make system interoperable with systems in other states.
- The ISS should have minimal delay with respect to data refresh from the data source(s).
- The query capability of the ISS should be flexible with respect to query input parameters.
- The query process of the ISS should be designed to enable the user to retrieve as much relevant data as possible via a single query.
- The ISS design should support a single metadata model.

- The ISS design should implement a single sign-on in conjunction with other systems with which it interfaces.
- The ISS functionality should not be designed to eliminate law enforcement roles or to replace law enforcement intuition with automated processes.
- The ISS should incorporate analytical tools with enough sophistication to deal with invalid or unconditioned data.
- The ISS should be designed to include a capability to perform link association among persons.
- The ISS design should specify a unique identifier to connect incidents with people through link analysis.
- The ISS should be designed to avoid the need to reenter query parameters on online forms when modifying a previously executed query.
- The ISS should be designed with end-user participation and subject-matter expertise in law enforcement.
- The ISS should include a help button feature.
- Implement a system that can provide a user query capability that enables a user to easily specify and modify query parameters.

4.3.5 Patrol Officer Recommended System Features

Depending on the purpose of the ISS, some organizations may choose to provide data to patrol officers. The interviewed ISS representatives provided the following lessons learned that will facilitate the use of ISS functions based on the patrol officer's role in the law enforcement business processes.

- Provide additional details for a person query (e.g., prior arrests/prior offenses, where last arrested).
- Provide address query providing what incidents occurred at the address, information on persons associated with the address, alerts for dangers at address (e.g., drug house).
- Provide color DMV driver's license photos.
- Implement mug shot display and pawn data access capabilities.
- Provide on demand alerts and BOLOs for patrol officers—for instance, when shift starts.
- Field officers benefit from a user interface that pre-populates query requests with appropriate search criteria and emphasizes drop-down menu selections.
- Tactical operations that utilize criminal activity maps to sweep target areas are more effective in clearing all types of warrants in those areas than by serving warrants individually in a wider graphic area.
- The system should enable case officers to disseminate case information to other personnel rather than having those personnel access information unknown to the case officer.
- A user feedback mechanism should be implemented to enable system successes to be recorded.
- A quality-control capability should be implemented that facilitates user data entry and performs validity checks.
- Ensure the validity of the source database(s) before acting on data.
- The ISS should support law enforcement personnel who are required to testify in court about how they arrived at their conclusions using data from the system.

4.3.6 Testing

Testing of an ISS often results in many lessons learned that should have been addressed in other phases of the system development lifecycle process. This section provides key items to consider when conducting testing of a new ISS.

- ISS testing should include individuals who understand the purpose and premise of beta testing.
- Testing of the ISS should be led by a test manager.
- The ISS should utilize automated test suites.
- Choose personnel interested in the system for beta testing to ensure quality feedback.
- Conduct a well-designed pilot test that encompasses all system functions to avoid user

burnout resulting from multiple, interim system builds.

- Test the system in a variety of agency environments utilizing multiple user test teams.
- Deploy a thoroughly tested system to avoid frustrating the end-user base.
- Beta testing should provide an indication of resources needed for deployment; resources for deployment should be increased initially to accommodate increased interest in new features.
- Each software release should go through adequate regression testing to ensure that the system functions correctly before replacing the operational release. (Regression testing is the rerunning of test cases that a program or application has previously executed correctly in order to detect errors created by changes or corrections made to the new version.)
- Sufficient test data from each participating agency is necessary for validating each release.
- It is essential to have participation in the testing by the full spectrum of users in a beta test prior to full release. The full range of users is necessary because the way in which these users interact with the system varies by their role and responsibilities. What one user might miss with respect to an application bug, another user might uncover through his/her very specific use of the system.

4.3.7 Training

Training is an important part of developing a new ISS. The interviewed ISS representatives all emphasized the importance of training to the overall program success. The following lessons learned from established ISS training efforts provide guidance for approaching, conducting, and organizing training on a new ISS.

- Achieve a high level of system effectiveness through adequate and mandatory initial user training and periodic refresher training courses.
- Create sufficient full-time training positions to meet the needs of the user base.
- Modify training to emphasize creation of link relationships.
- Training should emphasize to users the importance of reducing or eliminating the input of invalid data into the ISS.
- Training should explain the importance of entering success stories with respect to refresher training and future user training.
- User meetings help to solidify and refresh user training experience.
- Commitment from command staff is required to allot an adequate amount of training for their personnel.
- A dedicated training staff is needed to interact with and successfully train users.
- Implement a training plan to ensure that all users are trained effectively prior to using the system.
- Provide sufficient hardware/software resources to meet the requirements of the training plan.
- End-user commitment to using the system is required or training will prove to be ineffective.
- Evaluate training through feedback and comments from users to improve training.
- Methods of training for large number of officers need to be convenient and accessible. New approaches, such as making training programs available on closed circuit TV channels, is one approach that may be a solution. Another solution might be brief periodic newsletters.
- Training should occur shortly before the user is given access to the system. Training is often ineffective if it occurs well before the user has an opportunity to access the system.
- A training plan should define the requirements for refresher training needed in the event that the system user interface or capabilities change substantially in a subsequent release. Otherwise, users may misinterpret how the system functions, assume the new release is defective, and subsequently stop using the system.
- Small agencies should plan for conflicts of scheduling training, as scheduling training can be a difficult issue for agencies with a small agency IT staff and a large number of users.
- Training should be built into the system early in the project or implementation of the ISS.

4.3.8 Operations

Daily operations must have a set of standard operating procedures for users and administrators. The following lessons learned provided by the interviewed ISS representatives offer steps toward achieving a functioning ISS under optimal conditions.

- Agencies should plan to have sufficient resources to configure and maintain the hardware and software components needed for reliable and adequate access to the system. If users are discouraged from using the system due to any hardware/software issues, they will not appreciate how beneficial the system can be.
- Broadband wireless access from patrol cars should be implemented for practical use; commonly used commercial Cellular Digital Packet Data (CDPD) wireless service is not fast enough.
- The system should utilize as much current technology as possible and leverage its size and functionality to embrace newer technologies, such as wireless service.
- The ability to interface to other ISSs across the country eliminates information gaps and provides a more powerful law enforcement tool.
- Require that system-provided leads be vetted with the source agency before they can be used in criminal apprehensions or legal proceedings.
- Plan to upgrade system hardware every five years.
- Incorporate a remote software updating process for devices used in the field to avoid excessive costs of recalling equipment to implement the software update.
- Account for a dip in operational productivity due to a steep learning curve when transitioning to new technology(ies).
- Automate records management to reduce the headcount associated with manual recordkeeping.
- Timeliness of data returned is critical to creating actionable leads.
- Ability to run on mobile devices can increase the collaboration among investigative personnel, command staff, and officers in the field.
- Access to the ISS should be provided to the widest possible user base within member agencies in order to foster increased collaboration among those agencies.
- Participating agencies and users should understand the importance of reliable and accurate data entry.
- Create or add staff positions for the following key operational areas:
  - Data quality analysis
  - Systems administration
  - Test and development
  - Promotional presentations
- Implement a single system rather than several, disparate, multi-platform systems for cost-effectiveness.

4.3.9 System Promotion

While designing and implementing the ISS is important, so is advertising the features and functions that the new system will provide to regional users. Having a champion often is a critical lessons learned that ISS representatives believed was key to their continued operations. The champion and system proponents must continue to work with users to ensure they understand the purpose, capabilities, and proper operation of the system. The following lessons learned come from such a focus.

- There should be an internal public relations capability to disseminate success stories and evidence of system effectiveness to gain internal support among stakeholders and to provide for a steady funding source.
- Employee relations groups should be consulted when implementing an ISS.
- Use of the system should be tied to employee reviews as an incentive for users to accept and adapt to the system.
- Agency system advocates should be identified and required to champion projects and market the system internally.
- Do not underestimate the benefits that come from involving smaller agencies in the ISS program.

- Target the group of police officers with 7-14 years on the job, and convince them of the benefits of the system.
- ISS program advocates are needed to "sell the system" to prospective agencies.
- Focus stakeholders' attention on the big picture of the ISS program rather than minute details.
- Membership should be extended to other public safety organizations (e.g., fire departments and prosecutor offices) that could benefit from access to criminal subject or activity information.

Appendix A
Additional Reference Documents

Appendix A presents a list of all the cited reference documents.

A.1 Federal Documents

U.S. Department of Justice. 2000. *Privacy Impact Assessment for Justice Information Systems: Working Paper*. Washington, D.C. *www.ojp.usdoj.gov/archive/topics/integratedjustice/PIAFinal.pdf*

9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Official Edition) including the Executive Summary Stock Number: 041-015-00236-8 Author: National Commission on Terrorist Attacks Upon the United States (9-11 Commission) *www.9-11commission.gov/*

A.2 State, Local, ISS Documents

May 2005 *Presentation of FINDER Objectives*.

December 19, 2003 *Final ARJIS/SANDAG Consolidation Plan*.

A.3 Other Reference Documents

Zaworski, Martin J. *Assessing an Automated Information-Sharing Technology in the Post '9-11' Era: Do Local Law Enforcement Officers Think It Meets Their Needs?* January 2006.

Smith and Mosier. The MITRE Corporation. *Guidelines for Designing User Interface Software*. ESD-TR-86-278 August 1986. *http://hcibib.org/sam/index.html*

This page intentionally left blank

Appendix B
Interview and Survey Forms

Appendix B presents copies of the interview guideline and national survey forms.

B.1 Interview Agenda and Guide

This guide is separated into five general discussion areas. Each of these is geared to the specific areas of interest of the individuals who will be participating in the interviews. The minimum amount of time that the team anticipates will be needed to interview each group is also listed. The order of interviews may depend on the availability of the participants.

Discussion Area	Individuals Participating	Duration
High Level ISS Review	ISS Senior Management	2 hours
System Governance and Management	ISS Governance Board Representative	2 hours
System Functional Analysis	ISS Project Technical Manager and Member Agency IT Manager(s)	½ day
Member Agencies User Interviews	ISS Users from Participating Agencies	1 day
System Technical Analysis	ISS System IT and Management	½ – 1 day

The objective for this *Interview Agenda and Guide* is to enable the interview team to collect consistent data from each ISS. For each of the agenda items, a broad list of discussion topics has been developed from the prior materials and from the experience gained in the dry-run. The information collected will be documented in the ISS System Document for each ISS program interviewed. The information also forms the basis of the remaining CRISP products—*Statement of Requirements, Concept of Operations, Evaluation Factors and Metrics, and the CRISP Mapping Tool.*

The discussion topics are intended as a guide to facilitate discussions and elicit feedback. The discussions will focus on the interview participants; therefore, the guide is not intended to be a checklist. Not all topics are expected to be covered in an interview. Instead, the list of topics is to be used as a reminder of potential items to discuss where appropriate. Furthermore, it is likely that a person interviewed may wish to designate others for the discussion of certain topics.

For the Member Agency User Interviews a set of “questions” is provided. These are not intended to be read aloud and asked of the user; however, it is important that the full range of these topics be covered during these interviews.

High Level ISS Review: ISS Senior Management—2 Hours

System Background and History

- Who started effort, why, when? Was it a bottom-up effort?
- If started prior to 911 (or NCISP), any resultant ISS improvement initiatives (functions, policy, legal)?
- Funding sources development, amount expended to date?
- Funding sources operations, maintenance, new features, amount available, amount spent?
- Cost sharing arrangement(s)?
- Governance approach and documentation?
- MOU prior to sharing information?
- Security considerations (state, agency…) and need for audit trails?
- Legal considerations (local laws, FOIA, system certification…)?
- Privacy considerations?
- Roles of PD chiefs, government officials?
- How did the extent of technical knowledge of chiefs and government officers impact the ISS evolution?
- Approval requirements (city: manager, attorney, clerk, PD chief)?
- Development duration, IOC date, versions, current status?
- History of who operated system, where, and why?
- History of how governance, project, development, and operations staffed?
- History of requirements specification, RFP, contract award process for system acquisition?
- Developer—new development by vendor or university, commercial product?
- History of approach to design, implement, and test system?
- Status; research tool, system of record, probable cause determination?
- Keys to success?
- Pitfalls experienced? The most difficult hurdle?
- Lessons learned?

System Goals, Purpose, and Scope

- Objectives beyond improving public safety mission?
- Participants (local, state, federal, tribal)?
- Total number participating organizations, trend since inception?

Successes and General Analysis of Impact—System Effectiveness

- Public relations and ISS promotion approach?
- Success stories and effectiveness metrics?
- Positive impacts?
- What is the value added of the ISS?
- Negative impacts?
- Impediments to use?
- Use assessment (who uses the system most, least, why)?
- Use impact due to individual agency IT staff, resources, equipment, communications infrastructure?

National Criminal Intelligence Sharing Plan (NCISP) Recommendations

- Familiar with the NCISP?
- Use of, or ISS communications interoperable with, RISS, law enforcement officer (LEO), or SBU communications standards (# 21/22/24)?
- Used applying security practices to justice information-sharing guidance (#25)?

- Using Global Justice Extensible Markup Language (GJXML) (#26)?
- Vetting: background, fingerprints, criminal history check FBI/local, name-based record check every 3 years) (#27)?

Information Shared Regionally

- Law enforcement data sources (local, state, federal)?
- Intelligence data (28 CFR Part 23 compliance)?
- 28 CFR Part 23 adopted but not required?
- Non-law enforcement data sources (DMV, Commercial,…)?
- Total number of records accessible (e.g., 11 million)?
- Responsibility for data accuracy and currency?
- How, when are ISS data sources (centralized database, agency databases) updated?
- In general, how many years of historical data are available in the ISS data sources (e.g., limited such as 5 years of field interviews and 20 years of arrest data, or everything agency wants to (or can) provide)?

Jurisdiction and Agency Participants and Stakeholders

- Agency name, address, sworn # available (mapping)?
- Levels of participation, what levels, why?
- Data contribution required to participate? How much? What data?

Users and Beneficiaries

- Users (patrol, dispatcher, detective, crime analyst, intel analyst, command staff, non criminal justice users)?
- Total number of users?
- Typical min/max daily usage?
- Sworn and law enforcement agency employees?
- Vetting (background check, fingerprints, name-based check periodically…)?
- Levels of access capabilities and data (all transactions, juvenile…)?
- Supports agency CompStat process?
- Supports task forces such as monthly regional crime analyst meetings?
- Users access system directly or indirectly (users of another system perform a query that is automatically sent to the ISS, ISS results returned to system, system returns results to user)?
- User training approach?

Architecture, Network, and Communications

- Centralized ISS data warehouse networked with distributed agency data sources for updating warehouse, no data warehouse—network of distributed individual agency data sources?
- Types of agency data sources in the ISS network (agency RMS, agency data extracts in separate server…)?
- Approach to integration with agency data sources and access to data elements in data sources?
- Network for user access?
- Communications (state fiber intranet, internet, Frac T1, T1, 9.6…)?

Functionality

- Types of query transactions and intended users of each
- Text documents and Google-like searches?
- Other capabilities (e.g., Link Analysis) and Intended Users
- What works best?
- What does or didn't work?
- Desired capabilities?
- Who designed user interface and functionality?
- Who developed the requirements and were they documented in a requirements document?
- Does the ISS meet the objectives of the requirements document?

Overview of Operational Environment

- 24 x 7
- System typical response times (desktop, patrol car laptop with various wireless communications: broad band, CDPD …) and impacts to?
- Factors that impact system reliability, performance, usability?

Recommendations

- Critical success factors and metrics

System Governance and Management: ISS Governance Board Representative—2 hours

Governance Philosophy and Policies

- Organizational structure and reporting process?
- Approval process?
- Documentation and agreements?
- Who determined the scope of the system, what is it? Intrastate? Interstate?
- Lessons learned?

Roles and Responsibilities

- Executive board?
- Committees?
- PD chiefs?
- Agency government officials?
- Project management (one go-to-person)?
- Financial management (ISS funds)?
- Contract management (purchase, maintenance costs ISS software, hardware…)?
- System advocate?
- Single agency points of contact (attorney, project manager)?

Membership

- Application process?
- Voting and quorums?
- Voluntary membership termination?
- Involuntary membership termination?

Funding and Cost Considerations

- Initial funding?
- Continuance funding (e.g., operations, maintenance, and enhancements)?
- Budget planning?
- Cost-sharing?
- Expenditure approvals?

Incentives and Prerequisites for Participation

- What prerequisites are required for participation?
- Resources provided to the ISS?
- Funding provided to the ISS?
- Data provided to the ISS?

Legal Considerations

- Local, state, federal, tribal?
- Insurance for board members?
- Inter-state law enforcement data sharing?
- FOIA—ACLU, NRA?

Operations and Maintenance (O&M)?

- System certification and accreditation? Functional certification? Security certification? Who certified system—state, federal?
- Process for certification?
- Cost of certification?
- Defined critical success factors and metrics?
- How are metrics collected and related to success factors?

Planned Enhancements

Recommendations and Lessons Learned

- Governance?
- System promotion, success criteria, metrics?
- Procurement?
- Design?
- Implementation?
- Testing?
- User guides and system documentation?
- Training?
- Help desk?

System Functional Analysis: ISS Project Technical Manager and Member Agency IT Manager(s)—½ Day

System Architecture and Management

- Agency responsibilities?
- ISS responsibilities?
- Were there sufficient resources to develop the system?
- Were the requirements sufficient to meet user needs and policy needs?
- Did ISS get developed in line with requirements?
- Was there a particular architecture required to meet one or more agencies' enterprise architecture requirements?

Information Shared

- Arrests and bookings?
- Incident reports and narratives?
- Investigative reports and narratives?
- Field interview reports and narratives (criminal or intelligence data)?
- Tips and leads (intelligence data)?
- Traffic citations?
- Juvenile (A&B, Incident, Investigative, FI, Traffic)?
- Active warrants?
- Historical warrants?
- Stolen property?
- Evidence property?
- Pawn shop reports?
- Gang reports (criminal or intelligence data)?
- Adult mug shots?
- Juvenile mug shots (not typically shared)?
- Computer-aided dispatch (CAD)?
- Master name file?
- Master address file?
- Parking tickets?
- DMV color, grayscale, or B/W photos?
- DMV information?
- Commercial data sources (integrated into ISS)?
- Intelligence data sources (28 CFR Part 23 compliance required)?

Agency Data Sources/Database Integration

- Did agency's approach to providing data to the ISS need to comply with agency enterprise architecture?
- Approach (database architecture, standards, GJXML)?
- Where do data sources reside (agency RMSs, agency servers with replicated data, centralized database)?
- Data conversion activities?
- Who did the data conversion and data interface work (agency staff and vendor)?
- What are the agency responsibilities?

- What was the typical cost to an agency to provide data to the ISS (e.g., funds, staffing) for conversion, real time access, and updates?
- If distributed, estimate of staff hour (or $) effort for interfaces to agency data sources) for typical agency of small, medium, large size?
- If data centralized, estimate of staff hour (or $) effort for data extraction for typical agency of small, medium, large size?
- If data centralized, estimate of staff hour (or $) effort for creating ability to execute periodic data updates, and how often are updates done, pulled or pushed from agency sources?
- How long does it take to get an agency's data source integrated and available to the system?

Agency Network and Communications Integration

- Approach (enterprise architecture compliance, network and communications architecture, standards)?
- System security architecture?
- Who did the communications and networking work (agency staff and vendor)?
- What are the agency responsibilities?
- User administration (who does it and how)?
- Access control (username, password, other)? Meets CJIS Security policy guidelines for sharing of criminal history information?
- Single sign on (providing access to ISS and other systems)?
- Levels of data access authorization (restricted access to juvenile data, restricted access to certain features)?
- What did the agency provide and what was the cost to the agency?
- What did the ISS provide and who bore the cost, what was it?
- How long does it take to build the communications infrastructure and get it on line?

Concept of Operations -- Functional Capabilities Provided to Users

- Was there a CONOPS document?
- Use mandated?
- Transaction types provided to patrol officers?
- Transaction types provided to dispatchers?
- Transaction types provided to detectives/investigators?
- Transaction types provided to crime analysts?
- Transaction types provided to intelligence analysts?
- Transaction types provided to command staff, others?
- Analytical features?
- Mapping features (geo-coding)?
- Audit features?
- Other features?
- Can the number of active users be determined? How?

Training

- Training approach (Sunday morning, train the trainer, mentoring…)?
- Different training for different types of users?

Operations and Maintenance

- Functional capabilities?
- Enhancements?
- Audits (used for ISS abuse investigations, external)?
- Adequate level of service (ongoing system performance assessment capability)?

ISS Integration with National Initiatives/Systems

- RDeX (FBI Regional Data Exchange)?
- NDex (FBI National Data Exchange)?

ISS Integration with other Regional Initiatives/Systems

Obsolete Capabilities Previously Provided

- Functions not target to correct consumer?
- Resistance to change?

New Capabilities in the Planning Stage

Member Agencies User Interviews—1 Day (with participants from multiple agencies)

Operational Use Demonstrations and Discussions

- Agency Patrol Officer—2 hours
- Crime Analyst—2 hours
- Investigator/Detective—2 hours
- Intelligence Analyst—2 hours
- Command Staff—2 hours
- Others as appropriate—2 hours

Relevance of system to the user:

- What activities do you do in your daily job (e.g., vehicle stops, incident dispatches, arrests, case investigations, drug or gang activity intelligence investigations...)?
- How often did you use the system to assist you in your last 10 of these “activities”? (ask for each type of activity the person performs)
- How many of your last 10 of these “activities” did the system provide substantial assistance?
- How many of your last 10 of these “activities”, could there have been a possible negative experience or outcome without the assistance provided by the system?
- How many hours a day do you use the system? When do you use it?
- Are you required to use the system (mandated), if so is that a good idea, if not do you think you and your co-workers should be required to use it?

Positive impacts and features used:

- Does using the system save you time? Doing an “activity”, how long did it take without the system? How long with the system?
- Does the results obtained from using the system justify the time expended?
- For the patrol officer, does the system contribute to officer safety, if so, why?
- Does using the system give you an advantage you did not have previously? Describe specific positive impacts (e.g. found expired warrant on sex abuse in another agency, supports current sex abuse charge; determined persons actual name, commonly used aliases and several potential addresses used in other jurisdictions and was able to arrest person)
- Rank the transactions you use from most to least used
- Why do you use a specific transaction, what does it help with (e.g., vehicle license plate query helps with …)?
- Which of the query fields do you use most for each transaction you use, which are rarely used, why?
- For the patrol officer, does using the system change the way in which you work with the dispatcher?
- Which of the data fields that are returned in the response are most useful, least useful, why?
- Did the use of the system cause you to initiate collaboration with others in your or external agencies? Why, with whom?
- For the detective and analysts, can you estimate the number of positive outcomes in a month (e.g., case closures, arrests, successful intelligence operations) that can be attributed directly to using the information from the system that might not have been possible without the system? If this is hard to estimate, how would your agency be able to start collecting this information?

Negative impacts and impediments to using the system:

- If you are not using the system, why not?
- At times, can using the information provided by the system (or using the system) put you or someone in danger, why, how?
- Can using the system be frustrating to use, why, when?
- At times, is there too much information? When?
- Do you perceive that the information is sometimes inaccurate, or inconsistent?
- Are you cautious about using (or acting upon) information from other agencies because they have different data classification rules (e.g., they may enter something as a warrant that would not be a warrant in your agency) or they don't update the data as frequently as your agency (warrant may be expired)? Another reason?
- Is the system occasionally or frequently not accessible? Why, and does this affect you trying to use the system?
- Do you think the system is hard to use, was there any training, if so, was it adequate but you didn't have access to the system immediately after? Other reasons?

Ease of use:

- Is the system easy to use, if not, why not?
- Can you find the information you are looking for easily, if not, why not?
- Do you use a different system (RMS) rather than this system, if so, why?
- For the mobile user, do you prefer to ask the dispatcher than use the system directly?
- For the mobile user, does the system respond fast enough? Can you find what you need in the response quickly?
- Were you involved in designing the user interface of the system and functionality, if so, do you think that affects your ability to use the system?

Recommendations:

- What new query functions, other features, additional data would be desirable, if any, which is the most important to you?
- Need more or different training? Need a small handbook or cheat sheet?
- Do you have any ideas on how you can report on a regular basis when the system has really helped you so that the system will continue to receive the attention and funds necessary to make it even better?

System Technical Analysis—ISS System IT and Management Staff—½ – 1 day

- **Tour of ISS Operations (optional)**
- **Discussion Topics**

System Architecture:

System Hardware and Software:

System Networks and Communications Architecture:

System Data Stores/Database Architecture:

Ease of Integration with Agency Records Management Systems:

System Security Architecture:

System Performance:

System Reliability:

System Usability:

Use of Standards:

Automated Metrics Collection for System Effectiveness Evaluation?

Use of and Needs for Documentation:

Metrics

- How many users are registered to participate in the ISS? (Users and Beneficiaries Section)
- How many users are able to participate in the ISS?
  - Explain any difference in the two numbers above.
- What has been the annual growth rate in the number of participating users since ISS inception?
- How many agencies are participating in the ISS? (Users and Beneficiaries Section)
- How many agencies are able to participate in the ISS?
  - Explain any difference in the two numbers above.
- What has been the annual growth rate in number of participating agencies since ISS inception?
- What is the total number of records actually placed in the ISS? (Information-Sharing Regionally)
- What is the total number of records (estimated) that could be placed in the ISS?
  - Explain any difference in the two numbers above.
- What has been the annual growth rate in number of records placed in the ISS since ISS inception?

Requested ISS Documentation

As part of the CRISP Year 1 effort, copies of the following materials are requested, if available:

1. Background Information

□ Vision/Mission documents

□ Concept of Operations, Strategy, or feasibility documents

□ Original RFP, grant, or concept documentation

□ Presentations, briefings, or documents on history and evolution of the ISS

□ Organization charts, contact details: names, titles, phone numbers, email addresses

□ Electronic copy of ISS agency logos/patches

□ ISS marketing/executive summary brochures, flyers, documents

□ Map of ISS region and participating member jurisdictions

2. Governance Information

□ Copies of Memorandum of Understanding, Mutual Aid documents, Articles of Incorporation

□ Governance structure documents: organization charts, committees, decision making processes

□ List and briefly summarize profile of each member agency (#sworn staff, size of jurisdiction, population)

□ Documentation on how members join the ISS and their responsibilities

□ Information technology strategy plan: Per agency or for the entire ISS

□ Standard operating procedure document

□ Sample quarterly report

□ Capital Planning Process document

3. Existing System Information

☐ System documentation: network diagrams, application descriptions, communication lines

☐ List of databases used, file formats, as-built system documents

☐ System design documents, system user guides, system manuals

☐ Future roadmap, planned IT upgrades or project proposals

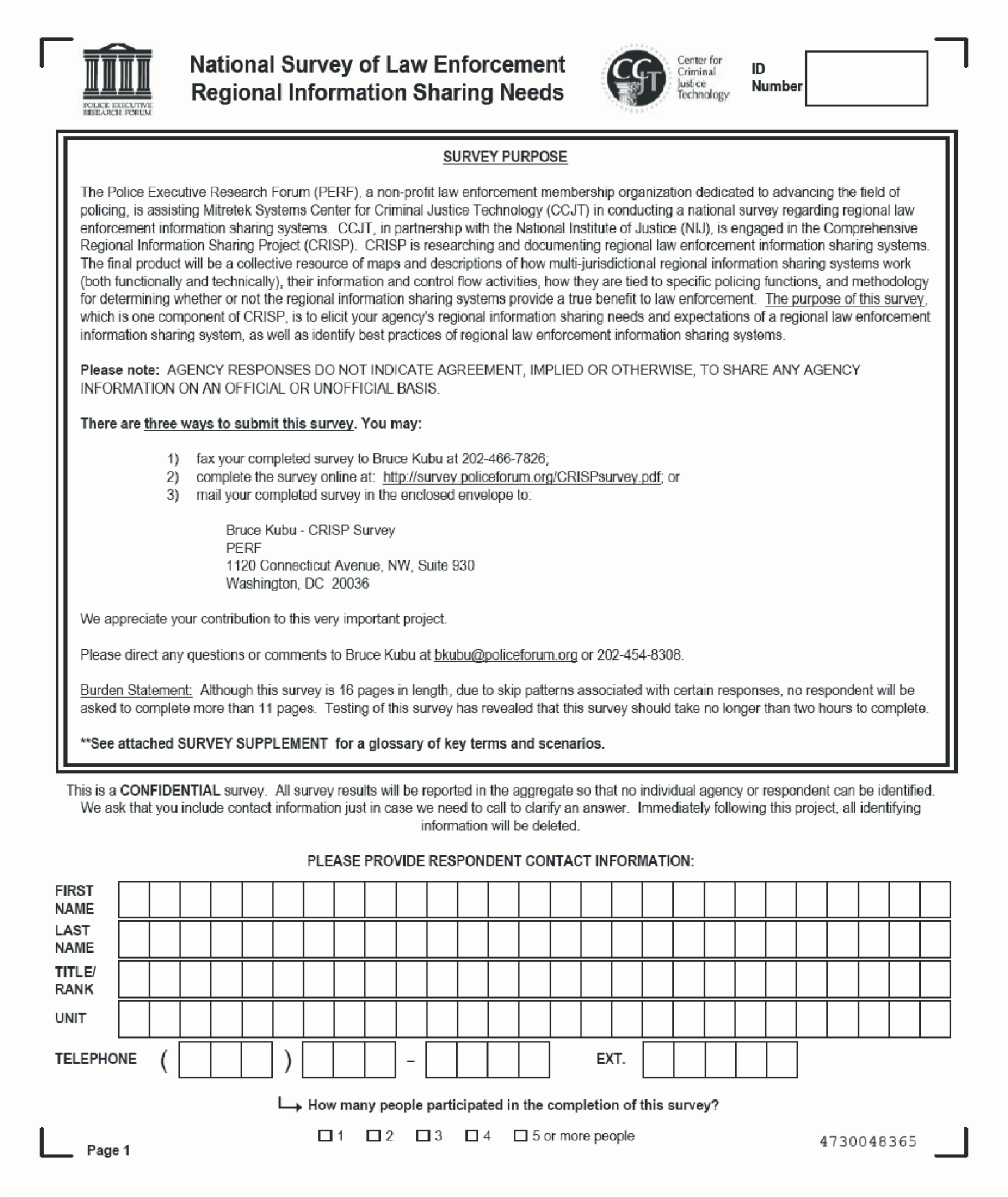
☐ Sample print outs of data entry screens

4. Blank Forms

☐ Governance Forms:

- Membership application
- Voting forms
- Other pertinent forms

B.2 National Survey Forms



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

SURVEY PURPOSE

The Police Executive Research Forum (PERF), a non-profit law enforcement membership organization dedicated to advancing the field of policing, is assisting Mitretek Systems Center for Criminal Justice Technology (CCJT) in conducting a national survey regarding regional law enforcement information sharing systems. CCJT, in partnership with the National Institute of Justice (NIJ), is engaged in the Comprehensive Regional Information Sharing Project (CRISP). CRISP is researching and documenting regional law enforcement information sharing systems. The final product will be a collective resource of maps and descriptions of how multi-jurisdictional regional information sharing systems work (both functionally and technically), their information and control flow activities, how they are tied to specific policing functions, and methodology for determining whether or not the regional information sharing systems provide a true benefit to law enforcement. The purpose of this survey, which is one component of CRISP, is to elicit your agency's regional information sharing needs and expectations of a regional law enforcement information sharing system, as well as identify best practices of regional law enforcement information sharing systems.

Please note: AGENCY RESPONSES DO NOT INDICATE AGREEMENT, IMPLIED OR OTHERWISE, TO SHARE ANY AGENCY INFORMATION ON AN OFFICIAL OR UNOFFICIAL BASIS.

There are three ways to submit this survey. You may:

1) fax your completed survey to Bruce Kubu at 202-466-7826;
2) complete the survey online at: http://survey.policeforum.org/CRISPsurvey.pdf; or
3) mail your completed survey in the enclosed envelope to:

Bruce Kubu - CRISP Survey
PERF
1120 Connecticut Avenue, NW, Suite 930
Washington, DC 20036

We appreciate your contribution to this very important project.

Please direct any questions or comments to Bruce Kubu at bkubu@policeforum.org or 202-454-8308.

Burden Statement: Although this survey is 16 pages in length, due to skip patterns associated with certain responses, no respondent will be asked to complete more than 11 pages. Testing of this survey has revealed that this survey should take no longer than two hours to complete.

****See attached SURVEY SUPPLEMENT for a glossary of key terms and scenarios.**

This is a **CONFIDENTIAL** survey. All survey results will be reported in the aggregate so that no individual agency or respondent can be identified. We ask that you include contact information just in case we need to call to clarify an answer. Immediately following this project, all identifying information will be deleted.

PLEASE PROVIDE RESPONDENT CONTACT INFORMATION:

FIRST NAME

LAST NAME

TITLE/ RANK

UNIT

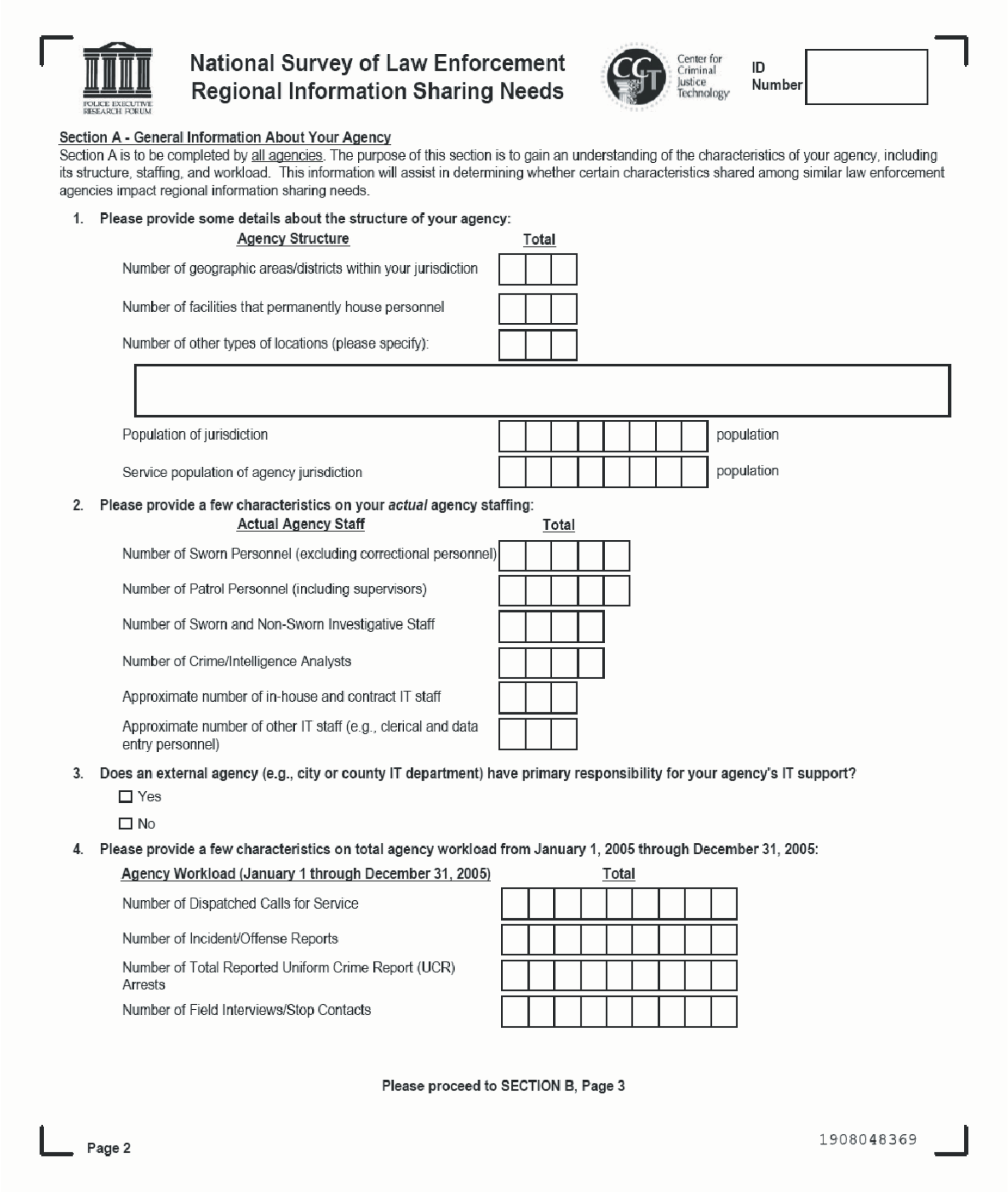
TELEPHONE ( ) - **EXT.**

How many people participated in the completion of this survey?

□ 1 □ 2 □ 3 □ 4 □ 5 or more people

Page 1

4730048365



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

Section A - General Information About Your Agency

Section A is to be completed by all agencies. The purpose of this section is to gain an understanding of the characteristics of your agency, including its structure, staffing, and workload. This information will assist in determining whether certain characteristics shared among similar law enforcement agencies impact regional information sharing needs.

1. **Please provide some details about the structure of your agency:**

Agency Structure	Total	
Number of geographic areas/districts within your jurisdiction		
Number of facilities that permanently house personnel		
Number of other types of locations (please specify):		
Population of jurisdiction		population
Service population of agency jurisdiction		population

2. **Please provide a few characteristics on your *actual* agency staffing:**

Actual Agency Staff	Total
Number of Sworn Personnel (excluding correctional personnel)	
Number of Patrol Personnel (including supervisors)	
Number of Sworn and Non-Sworn Investigative Staff	
Number of Crime/Intelligence Analysts	
Approximate number of in-house and contract IT staff	
Approximate number of other IT staff (e.g., clerical and data entry personnel)	

3. **Does an external agency (e.g., city or county IT department) have primary responsibility for your agency's IT support?**

   □ Yes

   □ No

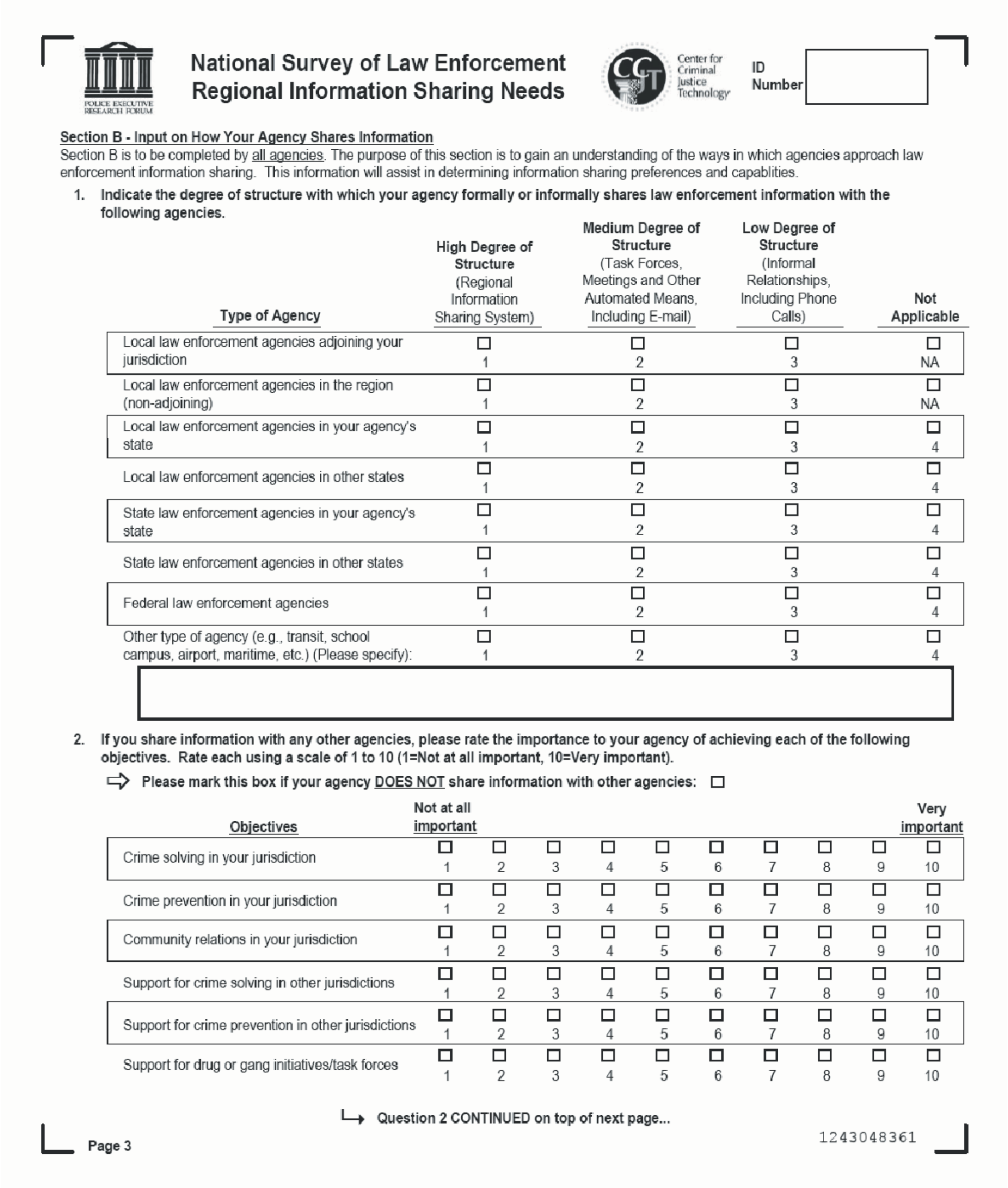
4. **Please provide a few characteristics on total agency workload from January 1, 2005 through December 31, 2005:**

Agency Workload (January 1 through December 31, 2005)	Total
Number of Dispatched Calls for Service	
Number of Incident/Offense Reports	
Number of Total Reported Uniform Crime Report (UCR) Arrests	
Number of Field Interviews/Stop Contacts	

Please proceed to SECTION B, Page 3

Page 2

1908048369



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

Section B - Input on How Your Agency Shares Information

Section B is to be completed by all agencies. The purpose of this section is to gain an understanding of the ways in which agencies approach law enforcement information sharing. This information will assist in determining information sharing preferences and capablities.

1. **Indicate the degree of structure with which your agency formally or informally shares law enforcement information with the following agencies.**

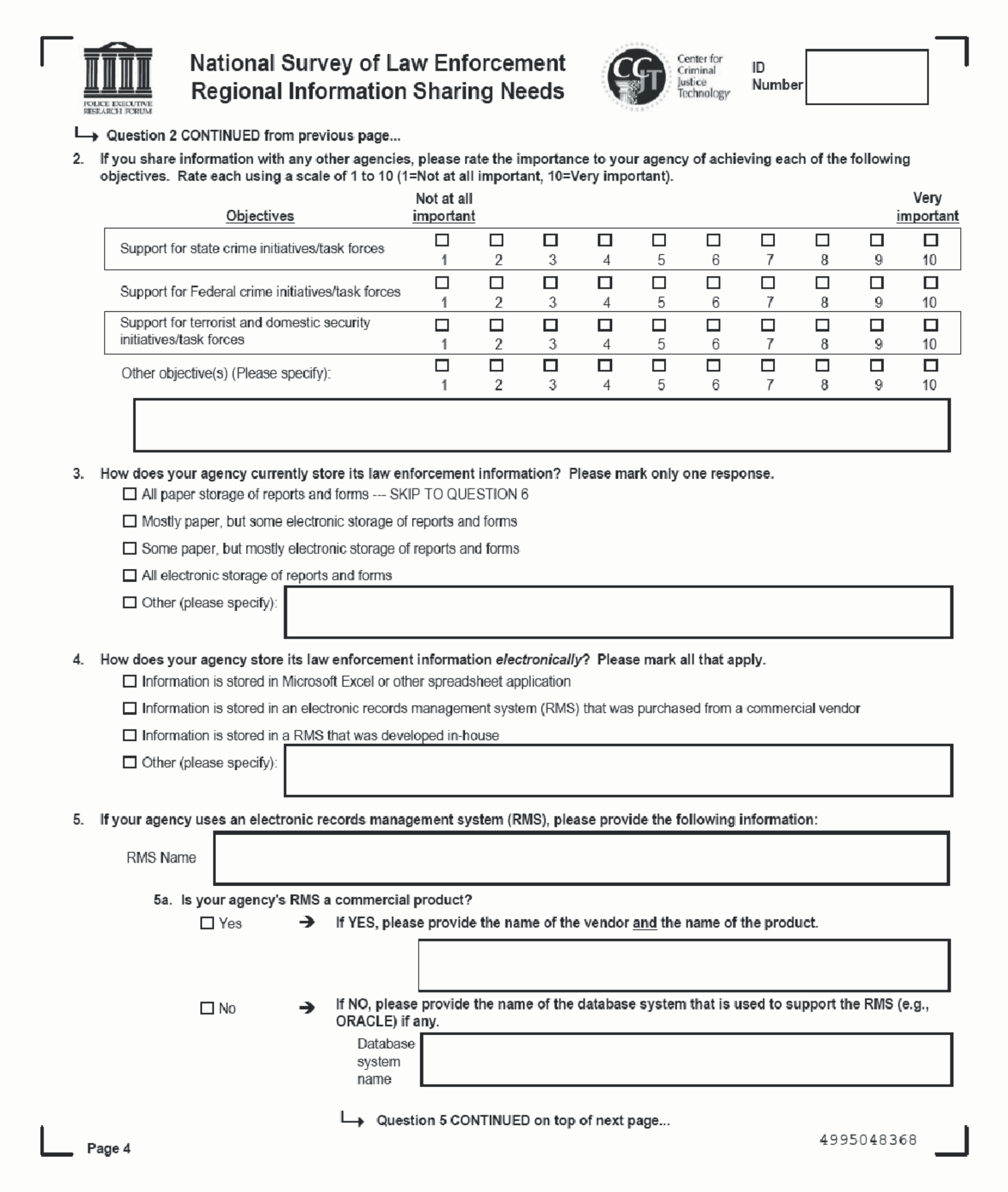
Type of Agency	**High Degree of Structure** (Regional Information Sharing System)	**Medium Degree of Structure** (Task Forces, Meetings and Other Automated Means, Including E-mail)	**Low Degree of Structure** (Informal Relationships, Including Phone Calls)	**Not Applicable**
Local law enforcement agencies adjoining your jurisdiction	□ 1	□ 2	□ 3	□ NA
Local law enforcement agencies in the region (non-adjoining)	□ 1	□ 2	□ 3	□ NA
Local law enforcement agencies in your agency's state	□ 1	□ 2	□ 3	□ 4
Local law enforcement agencies in other states	□ 1	□ 2	□ 3	□ 4
State law enforcement agencies in your agency's state	□ 1	□ 2	□ 3	□ 4
State law enforcement agencies in other states	□ 1	□ 2	□ 3	□ 4
Federal law enforcement agencies	□ 1	□ 2	□ 3	□ 4
Other type of agency (e.g., transit, school campus, airport, maritime, etc.) (Please specify):	□ 1	□ 2	□ 3	□ 4

2. **If you share information with any other agencies, please rate the importance to your agency of achieving each of the following objectives. Rate each using a scale of 1 to 10 (1=Not at all important, 10=Very important).**

⇨ **Please mark this box if your agency DOES NOT share information with other agencies:** □

Objectives	Not at all important									Very important
Crime solving in your jurisdiction	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Crime prevention in your jurisdiction	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Community relations in your jurisdiction	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Support for crime solving in other jurisdictions	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Support for crime prevention in other jurisdictions	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Support for drug or gang initiatives/task forces	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10

↳ **Question 2 CONTINUED on top of next page...**



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

Question 2 CONTINUED from previous page...

2. If you share information with any other agencies, please rate the importance to your agency of achieving each of the following objectives. Rate each using a scale of 1 to 10 (1=Not at all important, 10=Very important).

Objectives	Not at all important									Very important
Support for state crime initiatives/task forces	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Support for Federal crime initiatives/task forces	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Support for terrorist and domestic security initiatives/task forces	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Other objective(s) (Please specify):	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10

3. How does your agency currently store its law enforcement information? Please mark only one response.
   - □ All paper storage of reports and forms --- SKIP TO QUESTION 6
   - □ Mostly paper, but some electronic storage of reports and forms
   - □ Some paper, but mostly electronic storage of reports and forms
   - □ All electronic storage of reports and forms
   - □ Other (please specify):

4. How does your agency store its law enforcement information *electronically*? Please mark all that apply.
   - □ Information is stored in Microsoft Excel or other spreadsheet application
   - □ Information is stored in an electronic records management system (RMS) that was purchased from a commercial vendor
   - □ Information is stored in a RMS that was developed in-house
   - □ Other (please specify):

5. If your agency uses an electronic records management system (RMS), please provide the following information:

RMS Name

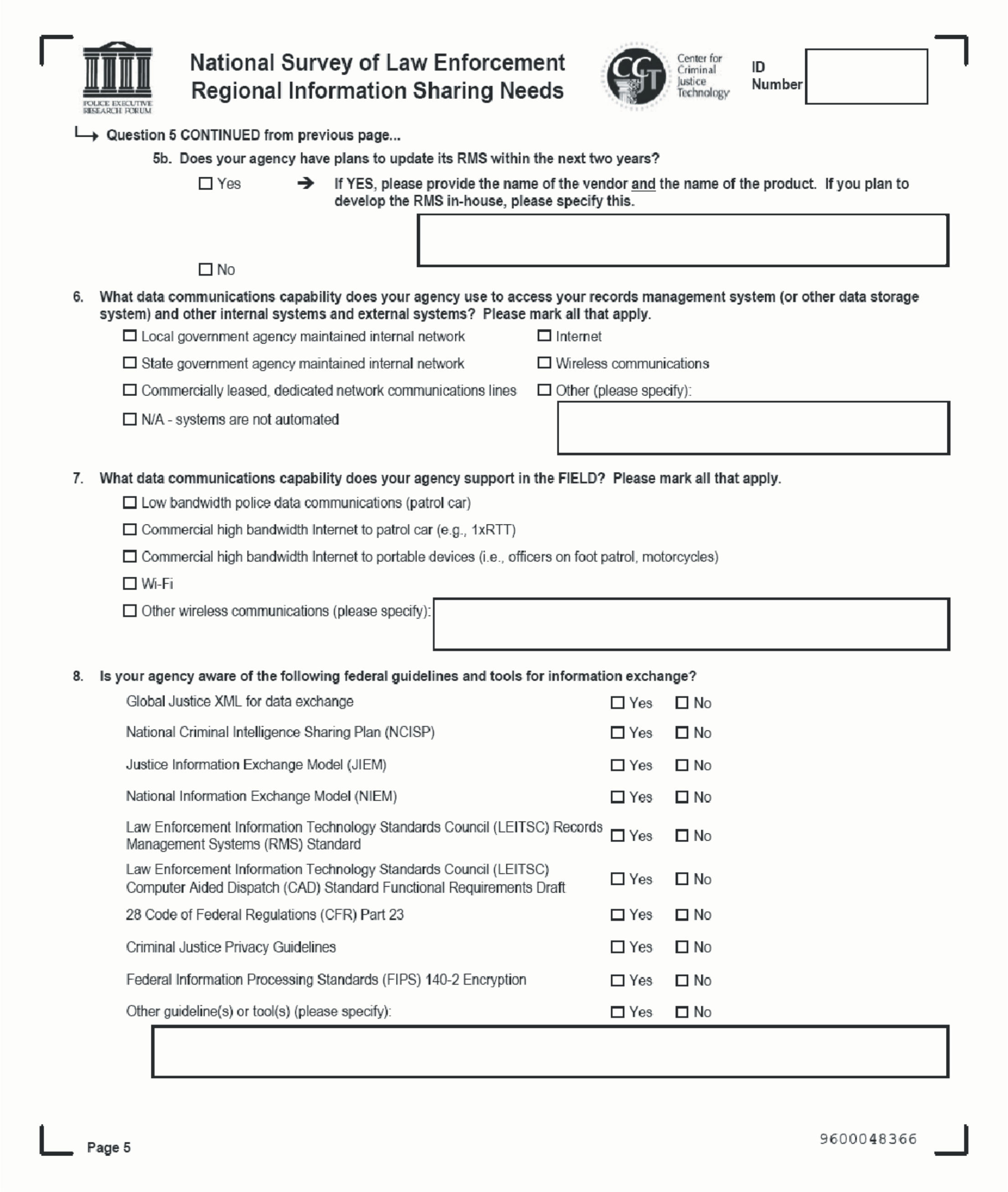
5a. Is your agency's RMS a commercial product?

□ Yes → If YES, please provide the name of the vendor <u>and</u> the name of the product.

□ No → If NO, please provide the name of the database system that is used to support the RMS (e.g., ORACLE) if any.

Database system name

Question 5 CONTINUED on top of next page...



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

└→ Question 5 CONTINUED from previous page...

5b. Does your agency have plans to update its RMS within the next two years?

□ Yes → If YES, please provide the name of the vendor and the name of the product. If you plan to develop the RMS in-house, please specify this.

□ No

6. What data communications capability does your agency use to access your records management system (or other data storage system) and other internal systems and external systems? Please mark all that apply.

□ Local government agency maintained internal network

□ State government agency maintained internal network

□ Commercially leased, dedicated network communications lines

□ N/A - systems are not automated

□ Internet

□ Wireless communications

□ Other (please specify):

7. What data communications capability does your agency support in the FIELD? Please mark all that apply.

□ Low bandwidth police data communications (patrol car)

□ Commercial high bandwidth Internet to patrol car (e.g., 1xRTT)

□ Commercial high bandwidth Internet to portable devices (i.e., officers on foot patrol, motorcycles)

□ Wi-Fi

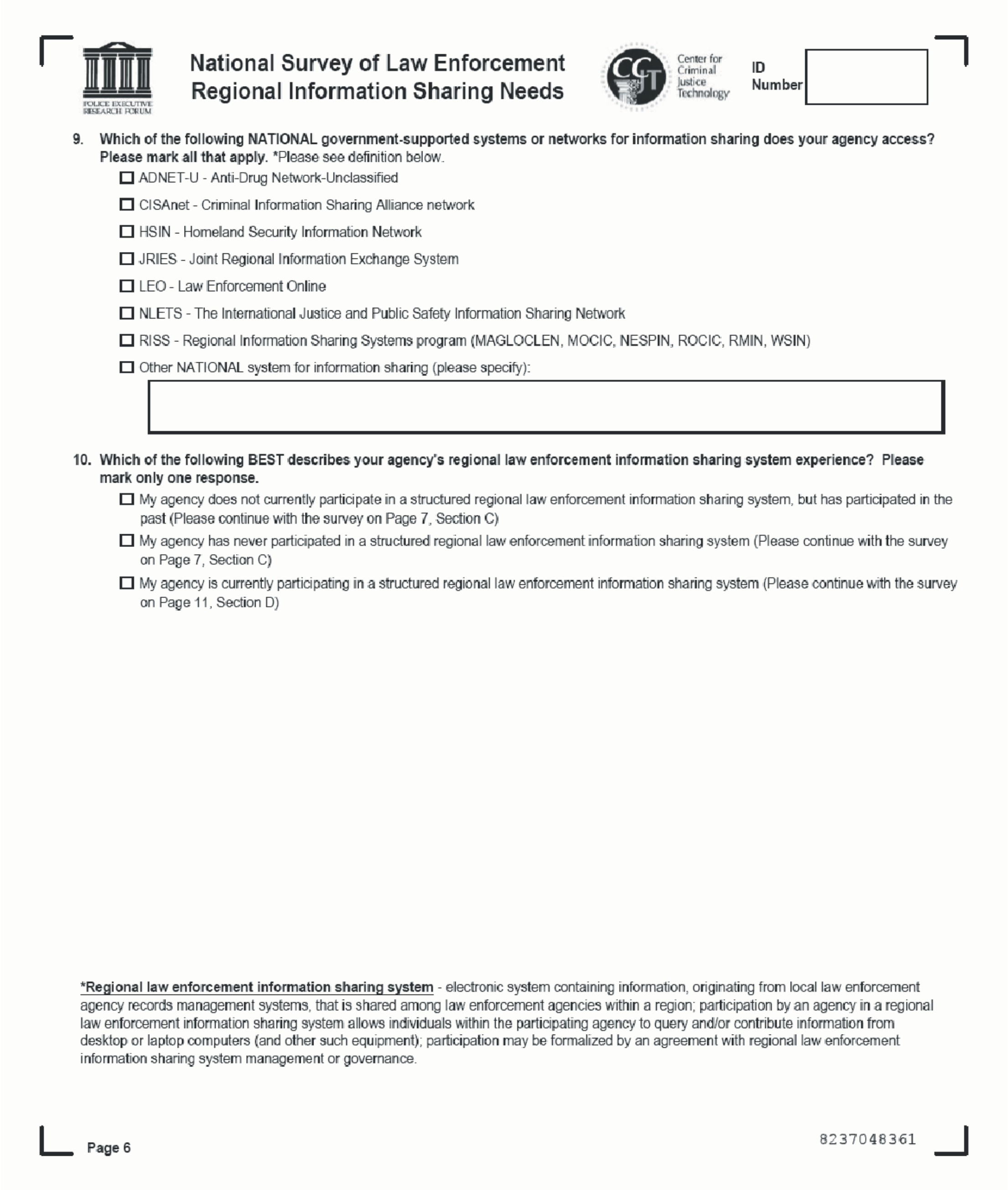
□ Other wireless communications (please specify):

8. Is your agency aware of the following federal guidelines and tools for information exchange?

Global Justice XML for data exchange	□ Yes	□ No
National Criminal Intelligence Sharing Plan (NCISP)	□ Yes	□ No
Justice Information Exchange Model (JIEM)	□ Yes	□ No
National Information Exchange Model (NIEM)	□ Yes	□ No
Law Enforcement Information Technology Standards Council (LEITSC) Records Management Systems (RMS) Standard	□ Yes	□ No
Law Enforcement Information Technology Standards Council (LEITSC) Computer Aided Dispatch (CAD) Standard Functional Requirements Draft	□ Yes	□ No
28 Code of Federal Regulations (CFR) Part 23	□ Yes	□ No
Criminal Justice Privacy Guidelines	□ Yes	□ No
Federal Information Processing Standards (FIPS) 140-2 Encryption	□ Yes	□ No
Other guideline(s) or tool(s) (please specify):	□ Yes	□ No

Page 5

9600048366



National Survey of Law Enforcement
Regional Information Sharing Needs

ID Number

9. **Which of the following NATIONAL government-supported systems or networks for information sharing does your agency access? Please mark all that apply.** *Please see definition below.

□ ADNET-U - Anti-Drug Network-Unclassified

□ CISAnet - Criminal Information Sharing Alliance network

□ HSIN - Homeland Security Information Network

□ JRIES - Joint Regional Information Exchange System

□ LEO - Law Enforcement Online

□ NLETS - The International Justice and Public Safety Information Sharing Network

□ RISS - Regional Information Sharing Systems program (MAGLOCLEN, MOCIC, NESPIN, ROCIC, RMIN, WSIN)

□ Other NATIONAL system for information sharing (please specify):

10. **Which of the following BEST describes your agency's regional law enforcement information sharing system experience? Please mark only one response.**

□ My agency does not currently participate in a structured regional law enforcement information sharing system, but has participated in the past (Please continue with the survey on Page 7, Section C)

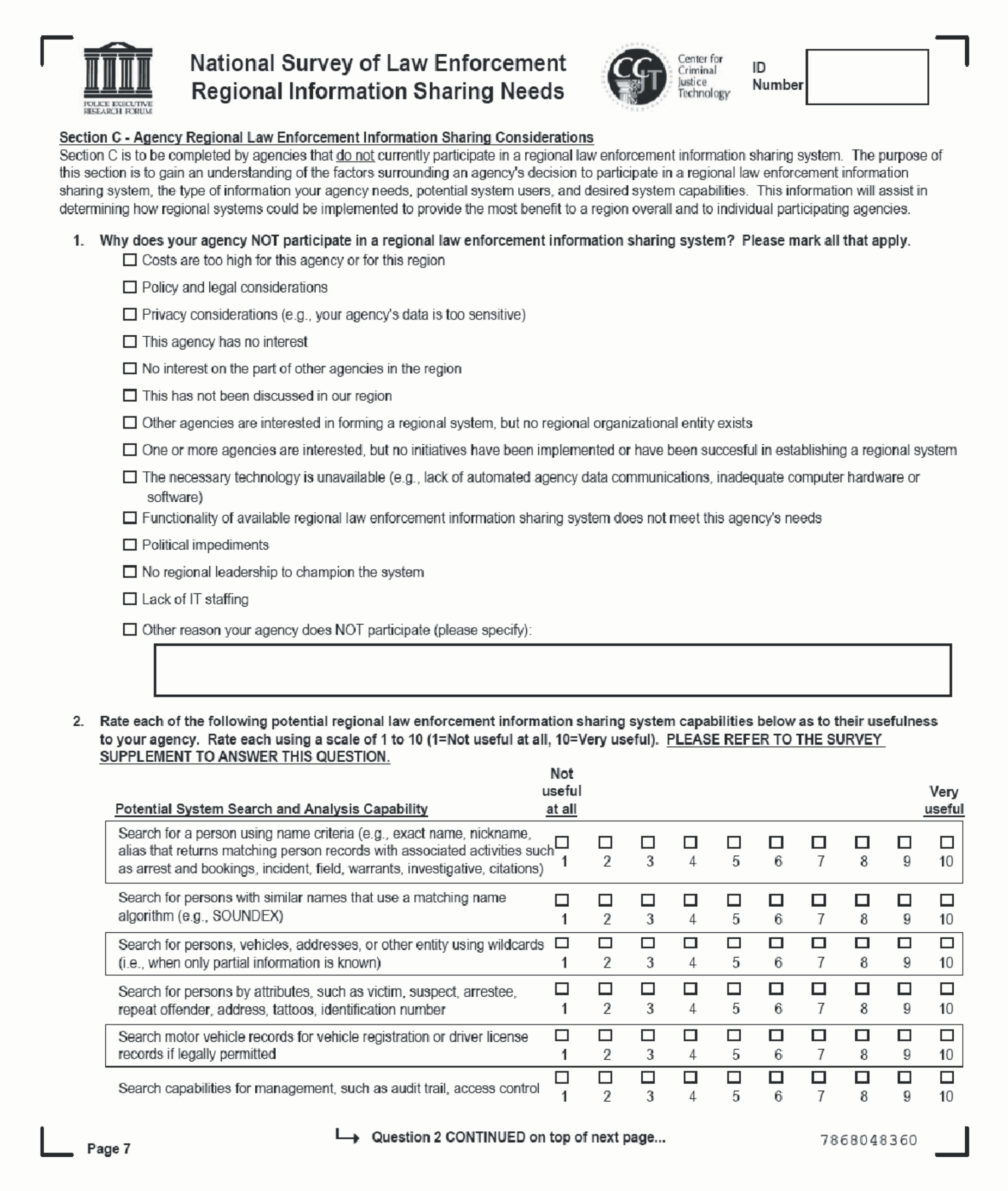
□ My agency has never participated in a structured regional law enforcement information sharing system (Please continue with the survey on Page 7, Section C)

□ My agency is currently participating in a structured regional law enforcement information sharing system (Please continue with the survey on Page 11, Section D)

***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.

Page 6

8237048361



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

Section C - Agency Regional Law Enforcement Information Sharing Considerations

Section C is to be completed by agencies that do not currently participate in a regional law enforcement information sharing system. The purpose of this section is to gain an understanding of the factors surrounding an agency's decision to participate in a regional law enforcement information sharing system, the type of information your agency needs, potential system users, and desired system capabilities. This information will assist in determining how regional systems could be implemented to provide the most benefit to a region overall and to individual participating agencies.

1. **Why does your agency NOT participate in a regional law enforcement information sharing system? Please mark all that apply.**

□ Costs are too high for this agency or for this region

□ Policy and legal considerations

□ Privacy considerations (e.g., your agency's data is too sensitive)

□ This agency has no interest

□ No interest on the part of other agencies in the region

□ This has not been discussed in our region

□ Other agencies are interested in forming a regional system, but no regional organizational entity exists

□ One or more agencies are interested, but no initiatives have been implemented or have been succesful in establishing a regional system

□ The necessary technology is unavailable (e.g., lack of automated agency data communications, inadequate computer hardware or software)

□ Functionality of available regional law enforcement information sharing system does not meet this agency's needs

□ Political impediments

□ No regional leadership to champion the system

□ Lack of IT staffing

□ Other reason your agency does NOT participate (please specify):

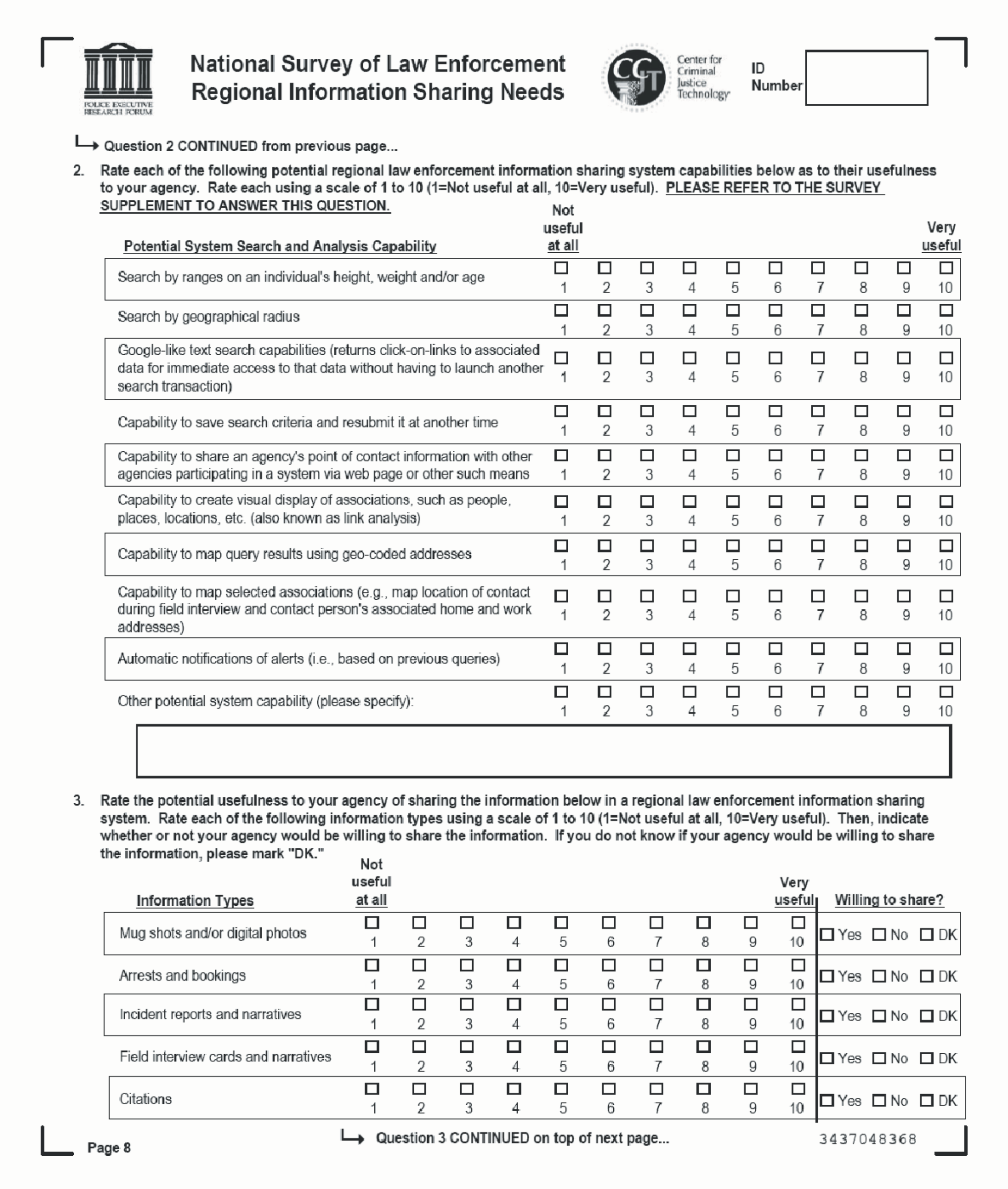
2. **Rate each of the following potential regional law enforcement information sharing system capabilities below as to their usefulness to your agency. Rate each using a scale of 1 to 10 (1=Not useful at all, 10=Very useful). PLEASE REFER TO THE SURVEY SUPPLEMENT TO ANSWER THIS QUESTION.**

Potential System Search and Analysis Capability	Not useful at all									Very useful
Search for a person using name criteria (e.g., exact name, nickname, alias that returns matching person records with associated activities such as arrest and bookings, incident, field, warrants, investigative, citations)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Search for persons with similar names that use a matching name algorithm (e.g., SOUNDEX)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Search for persons, vehicles, addresses, or other entity using wildcards (i.e., when only partial information is known)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Search for persons by attributes, such as victim, suspect, arrestee, repeat offender, address, tattoos, identification number	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Search motor vehicle records for vehicle registration or driver license records if legally permitted	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Search capabilities for management, such as audit trail, access control	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10

Page 7

↳ Question 2 CONTINUED on top of next page...

7868048360



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

↳ Question 2 CONTINUED from previous page...

2. **Rate each of the following potential regional law enforcement information sharing system capabilities below as to their usefulness to your agency. Rate each using a scale of 1 to 10 (1=Not useful at all, 10=Very useful). <u>PLEASE REFER TO THE SURVEY SUPPLEMENT TO ANSWER THIS QUESTION.</u>**

Potential System Search and Analysis Capability	Not useful at all									Very useful
Search by ranges on an individual's height, weight and/or age	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Search by geographical radius	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Google-like text search capabilities (returns click-on-links to associated data for immediate access to that data without having to launch another search transaction)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Capability to save search criteria and resubmit it at another time	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Capability to share an agency's point of contact information with other agencies participating in a system via web page or other such means	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Capability to create visual display of associations, such as people, places, locations, etc. (also known as link analysis)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Capability to map query results using geo-coded addresses	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Capability to map selected associations (e.g., map location of contact during field interview and contact person's associated home and work addresses)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Automatic notifications of alerts (i.e., based on previous queries)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Other potential system capability (please specify):	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10

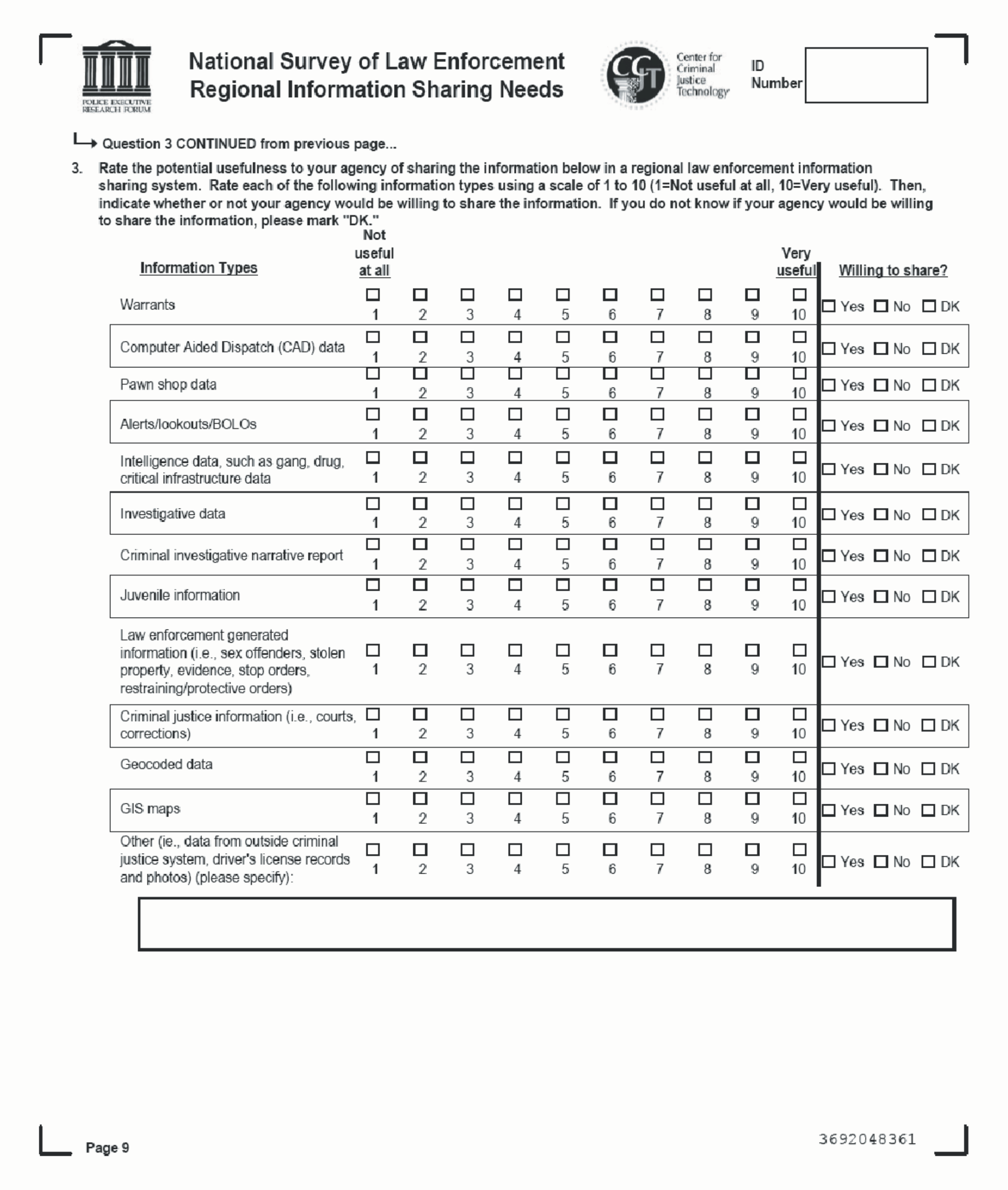
3. **Rate the potential usefulness to your agency of sharing the information below in a regional law enforcement information sharing system. Rate each of the following information types using a scale of 1 to 10 (1=Not useful at all, 10=Very useful). Then, indicate whether or not your agency would be willing to share the information. If you do not know if your agency would be willing to share the information, please mark "DK."**

Information Types	Not useful at all									Very useful	Willing to share?
Mug shots and/or digital photos	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Arrests and bookings	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Incident reports and narratives	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Field interview cards and narratives	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Citations	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK

Page 8

↳ Question 3 CONTINUED on top of next page...

3437048368



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

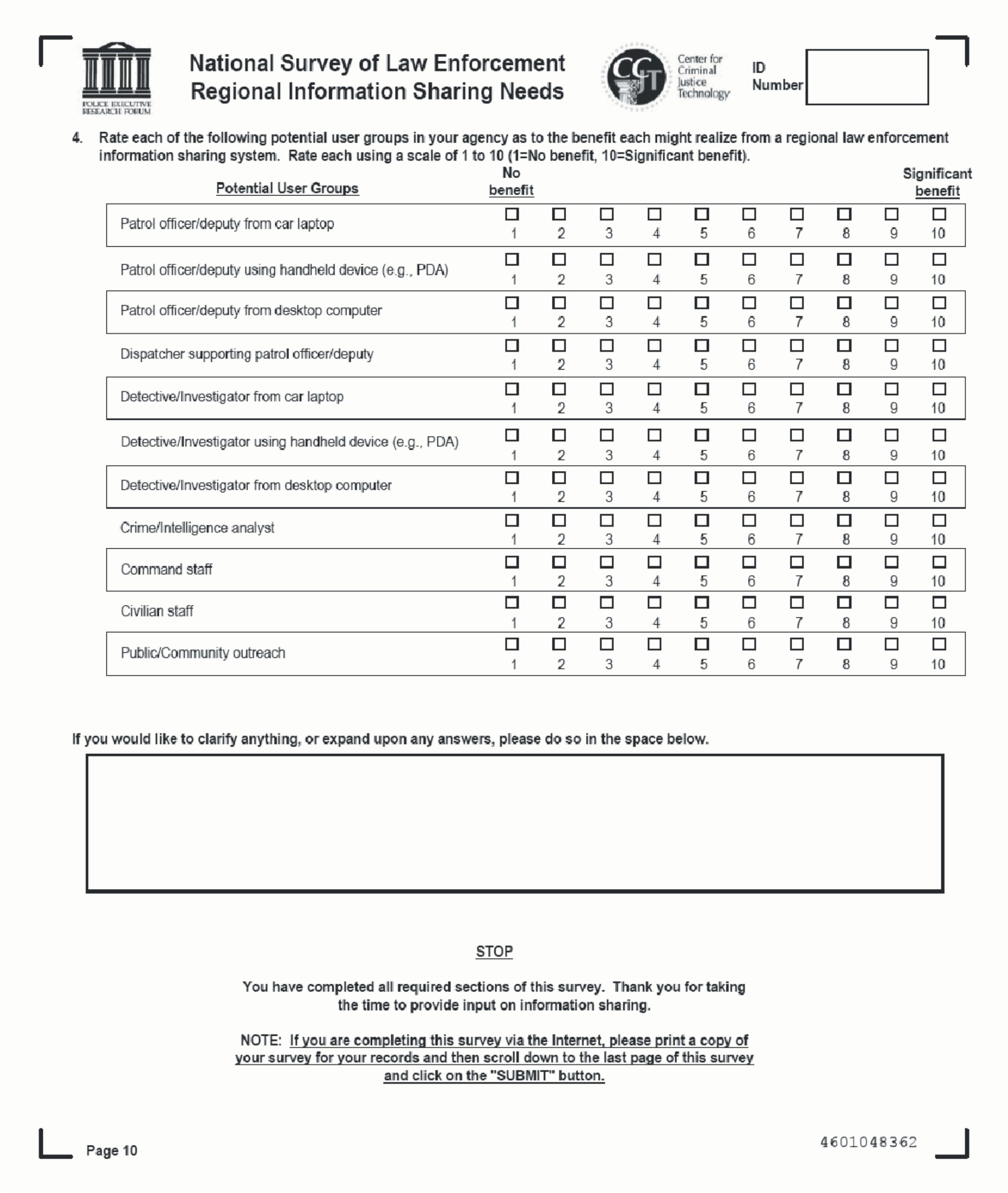
↳ Question 3 CONTINUED from previous page...

3. Rate the potential usefulness to your agency of sharing the information below in a regional law enforcement information sharing system. Rate each of the following information types using a scale of 1 to 10 (1=Not useful at all, 10=Very useful). Then, indicate whether or not your agency would be willing to share the information. If you do not know if your agency would be willing to share the information, please mark "DK."

Information Types	Not useful at all									Very useful	Willing to share?
Warrants	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Computer Aided Dispatch (CAD) data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Pawn shop data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Alerts/lookouts/BOLOs	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Intelligence data, such as gang, drug, critical infrastructure data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Investigative data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Criminal investigative narrative report	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Juvenile information	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Law enforcement generated information (i.e., sex offenders, stolen property, evidence, stop orders, restraining/protective orders)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Criminal justice information (i.e., courts, corrections)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Geocoded data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
GIS maps	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Other (ie., data from outside criminal justice system, driver's license records and photos) (please specify):	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK

Page 9

3692048361



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

4. Rate each of the following potential user groups in your agency as to the benefit each might realize from a regional law enforcement information sharing system. Rate each using a scale of 1 to 10 (1=No benefit, 10=Significant benefit).

Potential User Groups	No benefit									Significant benefit
Patrol officer/deputy from car laptop	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Patrol officer/deputy using handheld device (e.g., PDA)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Patrol officer/deputy from desktop computer	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Dispatcher supporting patrol officer/deputy	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Detective/Investigator from car laptop	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Detective/Investigator using handheld device (e.g., PDA)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Detective/Investigator from desktop computer	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Crime/Intelligence analyst	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Command staff	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Civilian staff	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Public/Community outreach	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10

If you would like to clarify anything, or expand upon any answers, please do so in the space below.

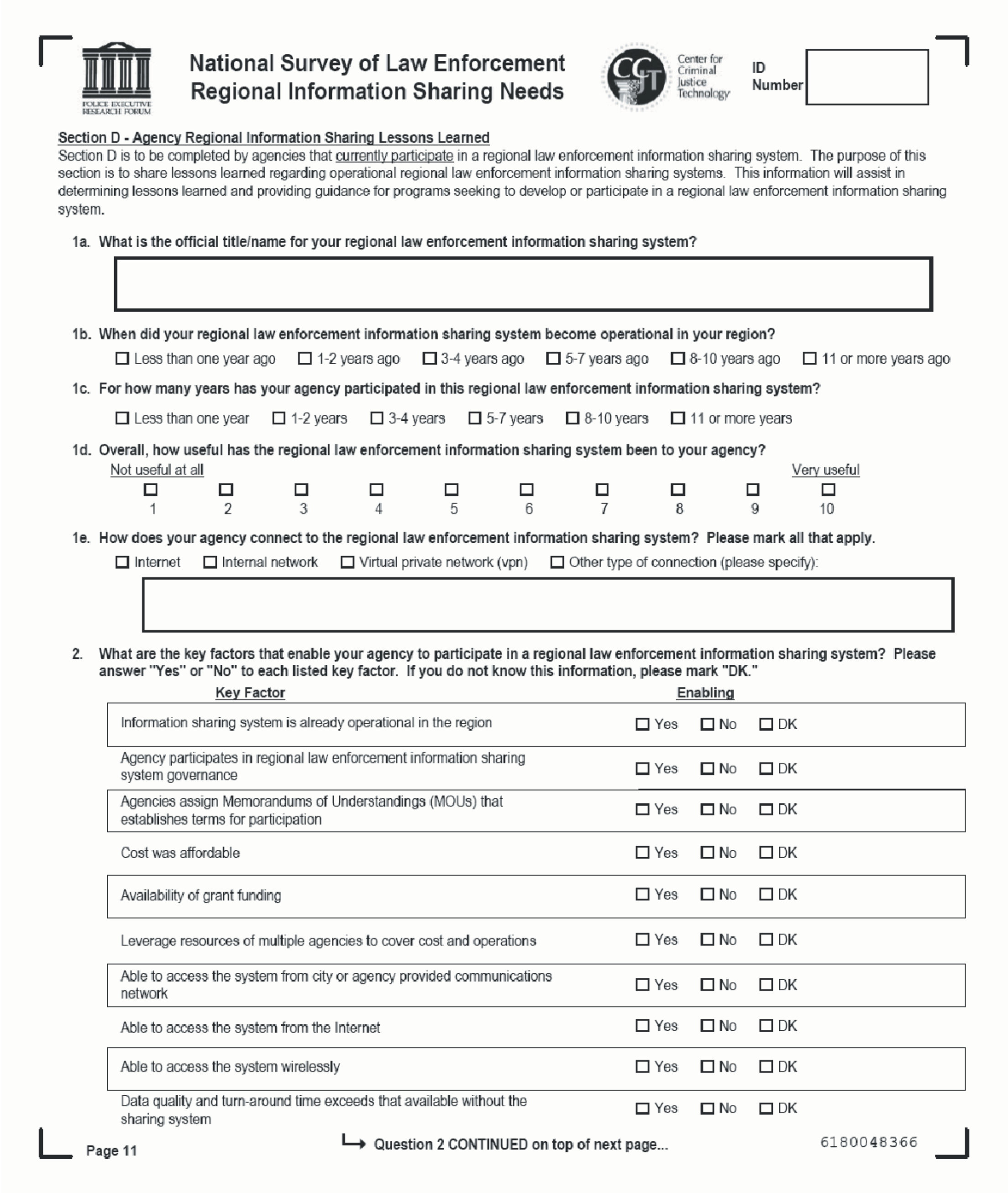
STOP

You have completed all required sections of this survey. Thank you for taking the time to provide input on information sharing.

NOTE: If you are completing this survey via the Internet, please print a copy of your survey for your records and then scroll down to the last page of this survey and click on the "SUBMIT" button.

Page 10

4601048362



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

Section D - Agency Regional Information Sharing Lessons Learned

Section D is to be completed by agencies that currently participate in a regional law enforcement information sharing system. The purpose of this section is to share lessons learned regarding operational regional law enforcement information sharing systems. This information will assist in determining lessons learned and providing guidance for programs seeking to develop or participate in a regional law enforcement information sharing system.

1a. What is the official title/name for your regional law enforcement information sharing system?

1b. When did your regional law enforcement information sharing system become operational in your region?

□ Less than one year ago □ 1-2 years ago □ 3-4 years ago □ 5-7 years ago □ 8-10 years ago □ 11 or more years ago

1c. For how many years has your agency participated in this regional law enforcement information sharing system?

□ Less than one year □ 1-2 years □ 3-4 years □ 5-7 years □ 8-10 years □ 11 or more years

1d. Overall, how useful has the regional law enforcement information sharing system been to your agency?

Not useful at all									Very useful
□	□	□	□	□	□	□	□	□	□
1	2	3	4	5	6	7	8	9	10

1e. How does your agency connect to the regional law enforcement information sharing system? Please mark all that apply.

□ Internet □ Internal network □ Virtual private network (vpn) □ Other type of connection (please specify):

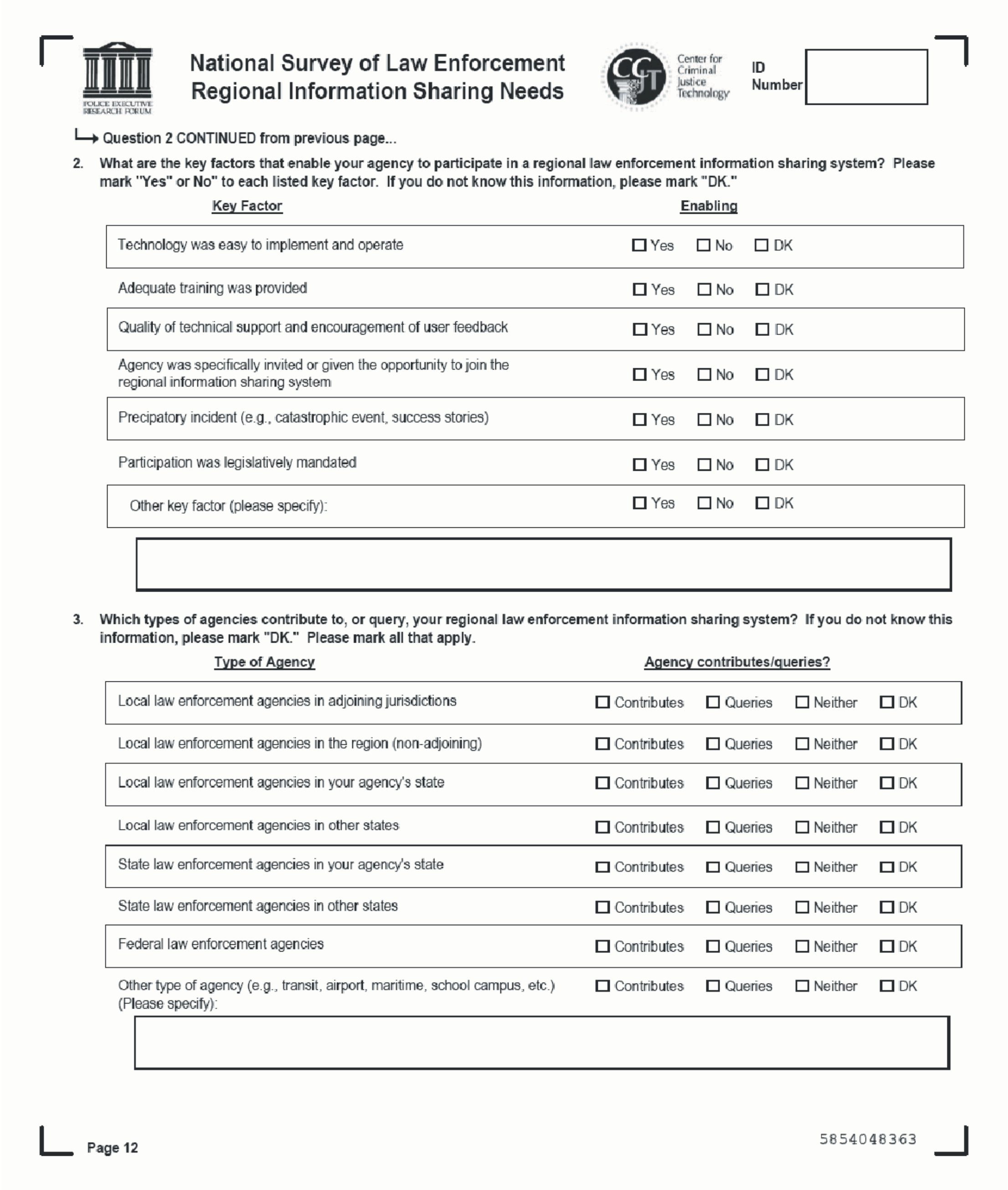
2. What are the key factors that enable your agency to participate in a regional law enforcement information sharing system? Please answer "Yes" or "No" to each listed key factor. If you do not know this information, please mark "DK."

Key Factor	Enabling
Information sharing system is already operational in the region	□ Yes □ No □ DK
Agency participates in regional law enforcement information sharing system governance	□ Yes □ No □ DK
Agencies assign Memorandums of Understandings (MOUs) that establishes terms for participation	□ Yes □ No □ DK
Cost was affordable	□ Yes □ No □ DK
Availability of grant funding	□ Yes □ No □ DK
Leverage resources of multiple agencies to cover cost and operations	□ Yes □ No □ DK
Able to access the system from city or agency provided communications network	□ Yes □ No □ DK
Able to access the system from the Internet	□ Yes □ No □ DK
Able to access the system wirelessly	□ Yes □ No □ DK
Data quality and turn-around time exceeds that available without the sharing system	□ Yes □ No □ DK

Page 11

Question 2 CONTINUED on top of next page...

6180048366



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

Question 2 CONTINUED from previous page...

2. What are the key factors that enable your agency to participate in a regional law enforcement information sharing system? Please mark "Yes" or No" to each listed key factor. If you do not know this information, please mark "DK."

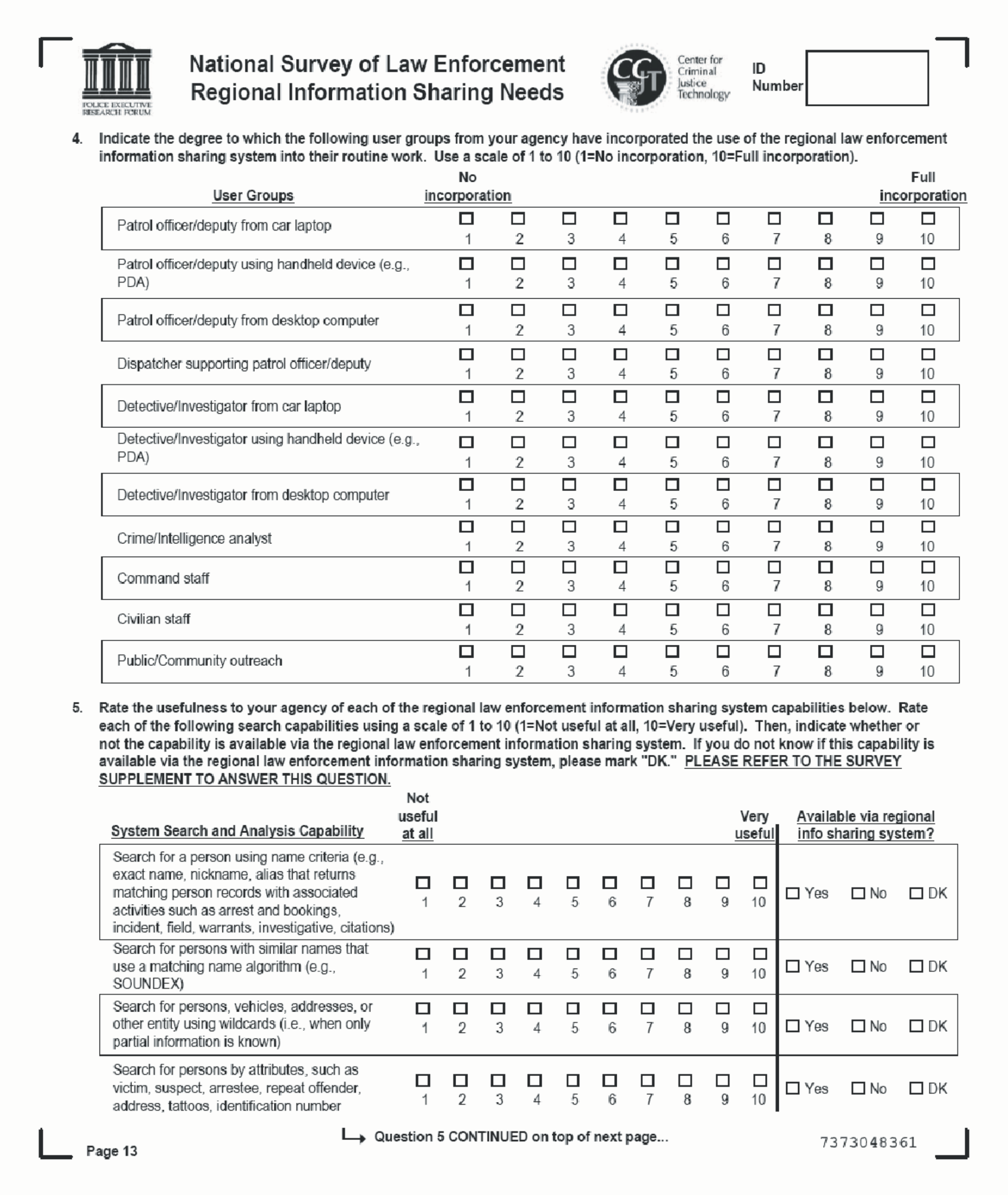
Key Factor	Enabling
Technology was easy to implement and operate	□ Yes □ No □ DK
Adequate training was provided	□ Yes □ No □ DK
Quality of technical support and encouragement of user feedback	□ Yes □ No □ DK
Agency was specifically invited or given the opportunity to join the regional information sharing system	□ Yes □ No □ DK
Precipatory incident (e.g., catastrophic event, success stories)	□ Yes □ No □ DK
Participation was legislatively mandated	□ Yes □ No □ DK
Other key factor (please specify):	□ Yes □ No □ DK

3. Which types of agencies contribute to, or query, your regional law enforcement information sharing system? If you do not know this information, please mark "DK." Please mark all that apply.

Type of Agency	Agency contributes/queries?
Local law enforcement agencies in adjoining jurisdictions	□ Contributes □ Queries □ Neither □ DK
Local law enforcement agencies in the region (non-adjoining)	□ Contributes □ Queries □ Neither □ DK
Local law enforcement agencies in your agency's state	□ Contributes □ Queries □ Neither □ DK
Local law enforcement agencies in other states	□ Contributes □ Queries □ Neither □ DK
State law enforcement agencies in your agency's state	□ Contributes □ Queries □ Neither □ DK
State law enforcement agencies in other states	□ Contributes □ Queries □ Neither □ DK
Federal law enforcement agencies	□ Contributes □ Queries □ Neither □ DK
Other type of agency (e.g., transit, airport, maritime, school campus, etc.) (Please specify):	□ Contributes □ Queries □ Neither □ DK

Page 12

5854048363



National Survey of Law Enforcement Regional Information Sharing Needs

ID Number

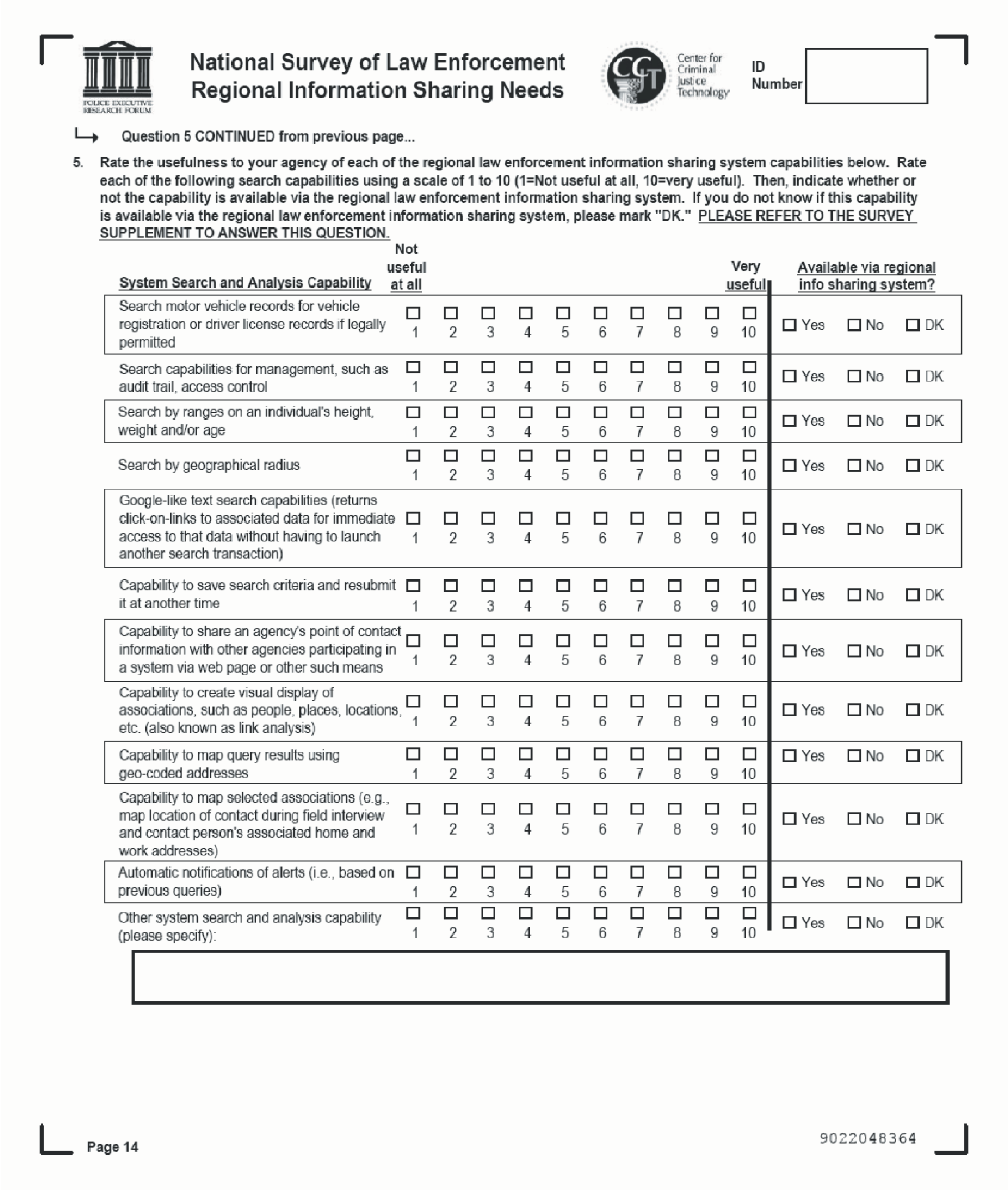
4. Indicate the degree to which the following user groups from your agency have incorporated the use of the regional law enforcement information sharing system into their routine work. Use a scale of 1 to 10 (1=No incorporation, 10=Full incorporation).

User Groups	No incorporation									Full incorporation
Patrol officer/deputy from car laptop	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Patrol officer/deputy using handheld device (e.g., PDA)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Patrol officer/deputy from desktop computer	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Dispatcher supporting patrol officer/deputy	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Detective/Investigator from car laptop	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Detective/Investigator using handheld device (e.g., PDA)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Detective/Investigator from desktop computer	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Crime/Intelligence analyst	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Command staff	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Civilian staff	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10
Public/Community outreach	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10

5. Rate the usefulness to your agency of each of the regional law enforcement information sharing system capabilities below. Rate each of the following search capabilities using a scale of 1 to 10 (1=Not useful at all, 10=Very useful). Then, indicate whether or not the capability is available via the regional law enforcement information sharing system. If you do not know if this capability is available via the regional law enforcement information sharing system, please mark "DK." PLEASE REFER TO THE SURVEY SUPPLEMENT TO ANSWER THIS QUESTION.

System Search and Analysis Capability	Not useful at all									Very useful	Available via regional info sharing system?		
Search for a person using name criteria (e.g., exact name, nickname, alias that returns matching person records with associated activities such as arrest and bookings, incident, field, warrants, investigative, citations)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Search for persons with similar names that use a matching name algorithm (e.g., SOUNDEX)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Search for persons, vehicles, addresses, or other entity using wildcards (i.e., when only partial information is known)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Search for persons by attributes, such as victim, suspect, arrestee, repeat offender, address, tattoos, identification number	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK

Question 5 CONTINUED on top of next page...



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

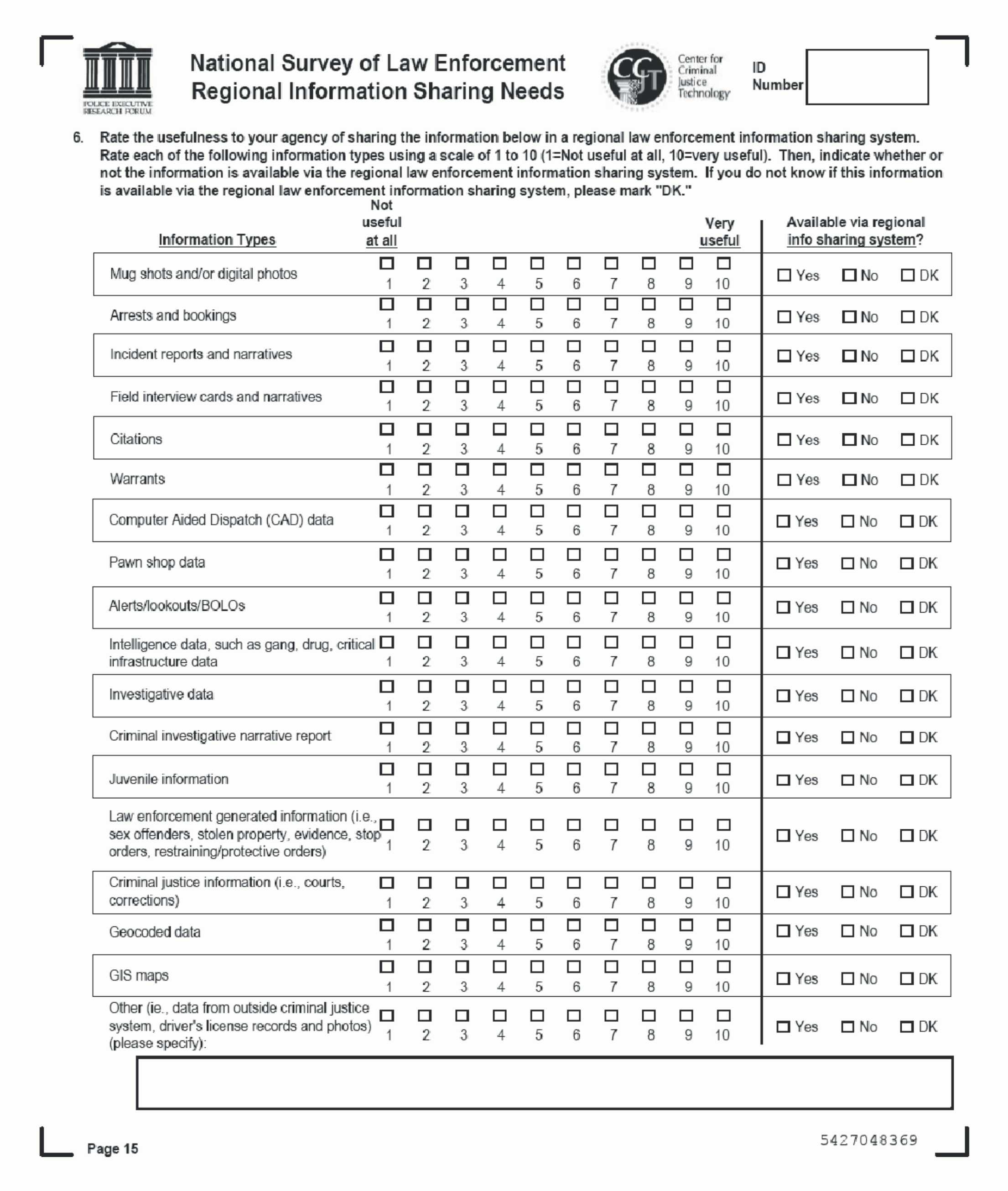
Center for Criminal Justice Technology

ID Number

↳ Question 5 CONTINUED from previous page...

5. Rate the usefulness to your agency of each of the regional law enforcement information sharing system capabilities below. Rate each of the following search capabilities using a scale of 1 to 10 (1=Not useful at all, 10=very useful). Then, indicate whether or not the capability is available via the regional law enforcement information sharing system. If you do not know if this capability is available via the regional law enforcement information sharing system, please mark "DK." PLEASE REFER TO THE SURVEY SUPPLEMENT TO ANSWER THIS QUESTION.

System Search and Analysis Capability	Not useful at all									Very useful	Available via regional info sharing system?		
Search motor vehicle records for vehicle registration or driver license records if legally permitted	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Search capabilities for management, such as audit trail, access control	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Search by ranges on an individual's height, weight and/or age	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Search by geographical radius	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Google-like text search capabilities (returns click-on-links to associated data for immediate access to that data without having to launch another search transaction)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Capability to save search criteria and resubmit it at another time	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Capability to share an agency's point of contact information with other agencies participating in a system via web page or other such means	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Capability to create visual display of associations, such as people, places, locations, etc. (also known as link analysis)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Capability to map query results using geo-coded addresses	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Capability to map selected associations (e.g., map location of contact during field interview and contact person's associated home and work addresses)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Automatic notifications of alerts (i.e., based on previous queries)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK
Other system search and analysis capability (please specify):	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes	□ No	□ DK



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

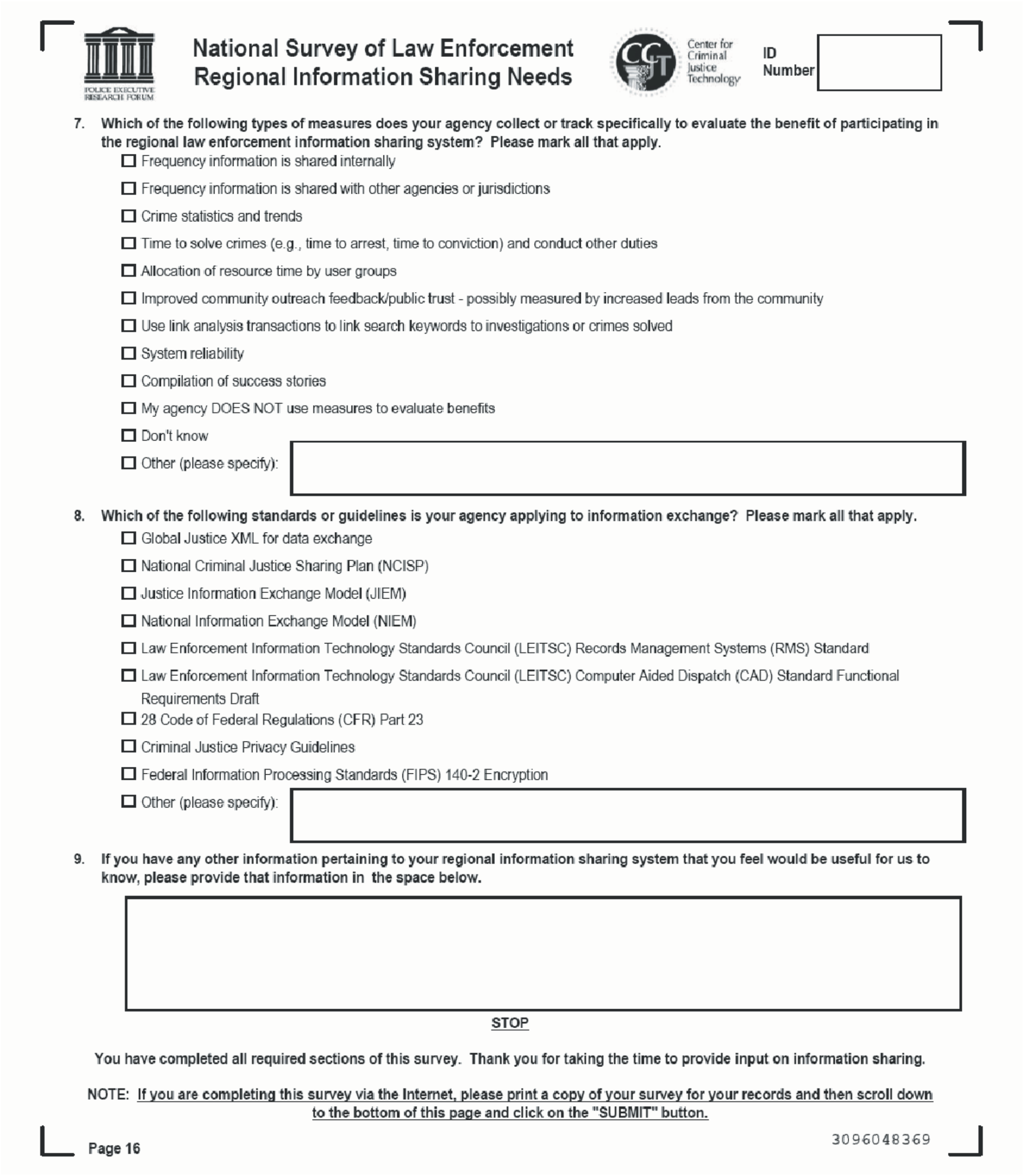
ID Number □

6. Rate the usefulness to your agency of sharing the information below in a regional law enforcement information sharing system. Rate each of the following information types using a scale of 1 to 10 (1=Not useful at all, 10=very useful). Then, indicate whether or not the information is available via the regional law enforcement information sharing system. If you do not know if this information is available via the regional law enforcement information sharing system, please mark "DK."

Information Types	Not useful at all									Very useful	Available via regional info sharing system?
Mug shots and/or digital photos	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Arrests and bookings	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Incident reports and narratives	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Field interview cards and narratives	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Citations	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Warrants	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Computer Aided Dispatch (CAD) data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Pawn shop data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Alerts/lookouts/BOLOs	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Intelligence data, such as gang, drug, critical infrastructure data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Investigative data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Criminal investigative narrative report	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Juvenile information	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Law enforcement generated information (i.e., sex offenders, stolen property, evidence, stop orders, restraining/protective orders)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Criminal justice information (i.e., courts, corrections)	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Geocoded data	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
GIS maps	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK
Other (ie., data from outside criminal justice system, driver's license records and photos) (please specify):	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9	□ 10	□ Yes □ No □ DK

Page 15

5427048369



POLICE EXECUTIVE RESEARCH FORUM

National Survey of Law Enforcement Regional Information Sharing Needs

Center for Criminal Justice Technology

ID Number

7. **Which of the following types of measures does your agency collect or track specifically to evaluate the benefit of participating in the regional law enforcement information sharing system? Please mark all that apply.**

□ Frequency information is shared internally

□ Frequency information is shared with other agencies or jurisdictions

□ Crime statistics and trends

□ Time to solve crimes (e.g., time to arrest, time to conviction) and conduct other duties

□ Allocation of resource time by user groups

□ Improved community outreach feedback/public trust - possibly measured by increased leads from the community

□ Use link analysis transactions to link search keywords to investigations or crimes solved

□ System reliability

□ Compilation of success stories

□ My agency DOES NOT use measures to evaluate benefits

□ Don't know

□ Other (please specify):

8. **Which of the following standards or guidelines is your agency applying to information exchange? Please mark all that apply.**

□ Global Justice XML for data exchange

□ National Criminal Justice Sharing Plan (NCISP)

□ Justice Information Exchange Model (JIEM)

□ National Information Exchange Model (NIEM)

□ Law Enforcement Information Technology Standards Council (LEITSC) Records Management Systems (RMS) Standard

□ Law Enforcement Information Technology Standards Council (LEITSC) Computer Aided Dispatch (CAD) Standard Functional Requirements Draft

□ 28 Code of Federal Regulations (CFR) Part 23

□ Criminal Justice Privacy Guidelines

□ Federal Information Processing Standards (FIPS) 140-2 Encryption

□ Other (please specify):

9. **If you have any other information pertaining to your regional information sharing system that you feel would be useful for us to know, please provide that information in the space below.**

STOP

You have completed all required sections of this survey. Thank you for taking the time to provide input on information sharing.

NOTE: If you are completing this survey via the Internet, please print a copy of your survey for your records and then scroll down to the bottom of this page and click on the "SUBMIT" button.

Page 16

3096048369

Appendix C Interview and Survey Methodology

This section provides an explanation of the interview methodology used by the CRISP team.

C.1 Data Collection Methodology

The CRISP team followed a set methodology in an attempt to employ an objective approach, as well as to collect a consistent set of data from interviewed and surveyed agencies. The methodology consisted of four key steps:

- Develop a list of representative operational information-sharing organizations to be interviewed and studied in depth
- Design a two-phased research approach
- Conduct a Phase One interview process
- Execute a Phase Two survey process

Figure C-1 illustrates the approach used.

C.1.1 Information-Sharing System Selection

Noblis identified seven ISS organizations as candidates for in-depth study and on-site interviews. The seven ISSs were selected from other potential ISS candidates because they shared a number of characteristics that were considered valuable to the CRISP study. The ISS had to be operational—not in the planning or development stage—and also had to be structured as one of the following:

- Comprised of one or more law enforcement agencies that had agreed to form an organization or signed a memorandum of understanding (MOU) or other agreement that enables sharing of specific information; the focus being the information rather than the communications network that supports the information-sharing
- Comprised of a regionally-based organization that provides management and systems support to the member law enforcement agencies

In addition to the criteria above, candidate ISSs were evaluated against the following four factors:

- Data access. The ISS should control, manage, or enable access to the shared information rather than just providing a pointer index to where the information is for later follow-up through another transaction or through telephone contact.
- Extent **of data sharing.** The ISS should allow participating agencies to share multiple types of law enforcement information, including CAD data, incident reports, and arrest reports.
- Investigator **support.** The ISS should support—or plan to support—investigators by providing analysis tools that help investigators analyze cases and other investigative information.

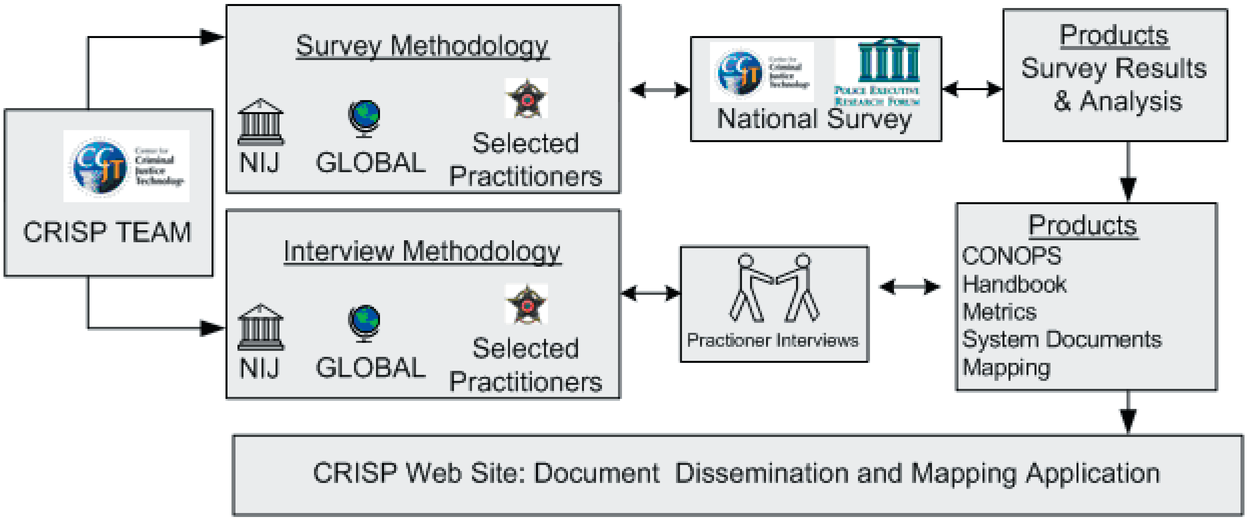


Figure C-1 CRISP Data Collection Approach

- **Patrol officer support.** The ISS should support—or plan to support—patrol officers by providing them access to ISS information from their patrol vehicles.

The selected ISS organizations are located in four regions of the county and vary in their size and structure and in the size of the population they serve. Each ISS organization appeared to be operational, mature, and stable in its operation and procedures. Several of the chosen ISS organizations had received awards from leading review publications, as well as recognition from the government. Many of the ISS organizations used federal grant funds to begin their efforts and were open to sharing their experiences in a manner that would benefit other law enforcement agencies interested in participating in or initiating a regional law enforcement ISS. Each ISS was provided the same background information, advance review material, and an MOU agreement that identified the objectives of CRISP and the responsibilities of Noblis and the participating agencies.

Time was spent early in the project developing materials to provide each candidate ISS with a clear understanding of the type and depth of information to be collected and of the estimated amount of time and staff resources that would be required during the interview process. In order to minimize the amount of time, the CRISP team also researched each ISS, gathering information from published sources prior to each on-site visit, then verifying the information during initial ISS meetings.

C.1.2 Two-Phased Research Approach

After identifying the ISSs to be interviewed in depth, the CRISP team developed a two-phased data collection and analysis approach to meet project goals. In the first phase, on-site interviews were conducted with each of the selected ISS organizations. The goal of the on-site interviews was to collect information about the respective ISS in five key discussion areas:

- High-Level ISS Review. Discussions were held with ISS senior management and covered the following areas:
  - System background and history
  - System goals, purpose, and scope
  - Successes and general analysis of impact—system effectiveness
  - NCISP recommendations
  - Information shared regionally
  - Jurisdiction and agency participants and stakeholders
  - Users and beneficiaries
  - Architecture, network, and communications
  - Functionality
  - Overview of operational environment
  - Recommendations
- **System Governance and Management.** Discussion were held with ISS governance board representatives and covered the following areas:
  - Governance philosophy and policies
  - Roles and responsibilities
  - Membership
  - Funding and cost considerations
  - Incentives and prerequisites for participation
  - Legal considerations
  - Operations and maintenance
  - Planned enhancements
  - Recommendations and lessons learned
- **System Functional Review.** Discussions were held with ISS technical management and member agency IT manager and covered the following:
  - System architecture and management
  - Information shared
  - Agency data sources and data integration
  - Network and communications access
  - Functional capabilities provided to users
  - Training
  - Operations and maintenance
  - ISS integration with national initiatives or systems
  - ISS integration with other regional initiatives or systems
  - New capabilities planned

- **ISS Member Agencies User Interviews.** Meetings were held with patrol officers, crime analysts, intelligence analysts, detectives/investigators, command staff, and others as appropriate to each ISS. Discussions covered the following:
  - Relevance of system to user
  - Positive impacts and features used
  - Negative impacts and impediments to using the system
  - Ease of use
  - Recommendations
- **System technical analysis.** Discussions were held with ISS technical or vendor staff, as available, and covered the following:
  - System architecture:
  - System hardware and software
  - System networks and communications architecture
  - System data stores/database architecture
  - Ease of integration with agency records management systems
  - System security architecture
  - System performance
  - System reliability
  - System usability
  - Use of standards
  - Use of and need for documentation

As can be seen from this comprehensive listing of topics, the evolution of the interview guide, provided in Appendix B, followed an iterative development process. Based on previous experiences and approaches, the persons to be interviewed needed to include a spectrum of users from the leadership to the patrol-officer level. Sections of the interview guide were designed to facilitate discussion with ISS senior managers, ISS governance board representatives, ISS project and participating agency technical managers, ISS users from participating agencies, and ISS system IT and management personnel. The CRISP team structured the guide to follow a typical system development lifecycle that started with the historical background for creating the system and then traced the system evolution up to present-day operations. The CRISP team conducted a dry-run interview in June 2005 with CRIMES ISS representatives and staff from participating agencies. Interview participants responded positively and provided feedback on how well the interviews covered law enforcement information-sharing topics. As a result of the dry run, the CRISP team made several improvements to the guide. The interview guide was then reviewed by representatives from GLOBAL and NIJ, and their recommendations were incorporated.

C.1.3 Phase One CRISP Interview Process

With the selected list of ISSs and completed interview material, the CRISP team focused on conducting the ISS site interviews, which were held September through November 2005. The ISSs were sent the interview material in advance to familiarize them with the type of information being solicited and to help them determine which staff should participate in interviews. A list of requested materials and documentation was also provided. Each ISS was asked to develop a list of participants and an agenda and to coordinate meetings that would take place over a two- to three-day period. The information stressed the need to provide users from as many participating agencies as feasible, this request proved to be one of the challenges of the interview process. In cases where staff from multiple agencies were able to attend, they provided insight into ISS effectiveness relevant to their tasks and frequently described unique ways in which the ISS supported them. The ISS also provided the team with consolidated sets of technical and other available pertinent documentation about the ISS.

The representatives and the interviewees from the participating agencies freely provided their recommendations and discussed areas of improvements from their unique experiences so that they could assist their counterparts in other agencies and regions. The participants would welcome further inquiries from practitioners. The system documents developed for each of the studied ISSs contain a complete list of individuals interviewed.

C.1.4 Phase Two CRISP National Survey Methodology

Phase Two involved a national survey of a broader base of representative law enforcement agencies throughout the country. Many of these agencies are not currently participants in regional ISSs. With the assistance of PERF, the CRISP team analyzed the survey results, which identified information-sharing needs and respective priorities. The results provided further support of the best practices gleaned from the Phase One interview data collection process. For more information on the national survey, please refer to the *PERF National Survey of Law Enforcement Regional Information-Sharing Needs* report.

Appendix D
Glossary of Terms and List of Acronyms

This appendix provide alphabetized list of acronyms found in this document. The terms that follow are defined in accordance with the context of this document and may have other meanings in other published documents.

D.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:

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

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.

System 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.

D.2 List of Acronyms

ARJIS	Automated Regional Justice Information System
BOLO	Be On the Lookout
CAD	Computer-Aided Dispatch
CCJT	Center for Criminal Justice Technology
CDPD	Cellular Digital Packet Data
CFR	Code of Federal Regulations
CLEAR	Citizen and Law Enforcement Analysis and Reporting
CONOPS	Concept of Operations
COPS	Community-Oriented Policing Services
COTS	Commercial-off-the-shelf
CPD	Chicago Police Department
CRIMES	Comprehensive Regional Information Management Exchange System
CRISP	Comprehensive Regional Information-Sharing Project
DEA	Drug Enforcement Agency
DOC	Deployment Operations Center
DOJ	Department of Justice
ETL	Extraction, translation, and loading
FAC	Federal Advisory Committee
FACTS	Factual Analysis Criminal Threat Solution
FBI	Federal Bureau of Investigation
FDLE	Florida Department of Law Enforcement

FINDER	Florida Information Network for Data Exchange and Retrieval
FOIA	Freedom of Information Act
GISP	Global Information-Sharing Plan
GJXML	Global Justice Extensible Markup Language
GUI	Graphical user interface
HIDTA	High-Intensity Drug Trafficking Area (Program)
IACP	International Association of Chiefs of Police
ICE	Immigration and Customs Enforcement
InSite	(Florida) Intelligence Site
ISS	Information-sharing system
IT	Information Technology
JAD	Joint application design
LEITSC	Law Enforcement Information Technology Standards Council
LEO	Law enforcement officer
MORE	Making Officer Redeployment Effective
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NCISP	National Criminal Intelligence Sharing Plan
NIJ	National Institute of Justice
NLETS	National Law Enforcement Telecommunications System
O&M	Operations and maintenance
PDA	Personal data assistant
PERF	Police Executive Research Forum
PSPAC	Public Safety Policy Advisory Committee
RMS	Records management system
SANDAG	San Diego Area Governments
SDLC	System development life cycle
SOP	Standard Operating Procedure
SPIN	Security Police Information Network
SQL	Structured query language
SSL	Secure Socket Layer
VPN	Virtual private network

This page intentionally left blank