

MONOGRAPH

**The
Statewide
Intelligence
Systems
Program**

September 1998



Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

This project was supported by Grant Number 95-DD-BX-0087, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

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

Institute for Intergovernmental Research
Post Office Box 12729
Tallahassee, Florida 32317

.....Table of Contents

Introduction	4
The Statewide Intelligence Systems (SIS) Program	6
Program Strategy and Implementation	9
Summary Descriptions of the SIS Projects	11
Tennessee Bureau of Investigation SIS Project.....	11
Wisconsin Department of Justice SIS Project	13
Connecticut State Police SIS Project	14
North Dakota Office of Attorney General SIS Project	15
Utah Department of Public Safety SIS Project.....	16
Lessons Learned	19
Appendixes	
Appendix A Statewide Intelligence System Sample Operating Policies and Procedures	24
Appendix B Criminal Intelligence Systems Operating Policies 28 CFR Part 23	34
Appendix C Statewide Intelligence System Control Group Sample Memorandum of Understanding.....	39
Appendix D Statewide Intelligence System Sample Participation Agreement.....	41

.....Introduction

Many state governments in the United States have established, or are in the initial stages of implementing, information systems for gathering, storing, and disseminating criminal intelligence information on a statewide basis. These information systems often vary greatly in their configuration, complexity, focus, and management. The purpose of the Statewide Intelligence Systems (SIS) Program—a federally funded grant award program—was to develop and facilitate replication of a statewide criminal intelligence-sharing model that maximized the effectiveness of shared management decisionmaking in the collection, storage, and dissemination of criminal intelligence information on a statewide basis.

This monograph has been prepared to assist the many state law enforcement and criminal justice agencies that are joining forces and sharing resources to combat multijurisdictional criminal activity through establishment of multijurisdictional criminal intelligence systems. Described herein are the steps necessary to successfully develop and implement a unique law enforcement criminal intelligence system—the model developed through the SIS Program. The information presented in this document should be useful to agencies involved in a wide range of multijurisdictional law enforcement intelligence-sharing efforts. Presented also are policies and procedures helpful for establishing and governing the operation of intelligence systems as well as the types of developmental problems encountered and the solutions attained.

The Tennessee Bureau of Investigation, the Wisconsin Department of Justice, the Connecticut State Police, the North Dakota Office of Attorney General, and the Utah Department of Public Safety acted as host agencies for their respective statewide intelligence system projects.

In summary, the monograph describes the experiences resulting from the initiation, development, and implementation of the SIS Program. The SIS Program received initial funding in 1993 from the Bureau of Justice Assistance (BJA). The program was subsequently awarded continuation funding. Federal funding support to all sites ended by April 1998. Representatives of states that are interested in replicating the statewide intelligence systems described in this monograph may contact the state agencies that participated in the SIS Program for technical specifications and additional information.

Program Links

The model intelligence system developed under the SIS Program was designed for compatibility with systems operated by the Regional Information Sharing Systems (RISS) Program Intelligence Centers (another program funded by BJA). The RISS Program Intelligence Centers support the exchange of criminal intelligence information among participating local, state, and federal law enforcement agencies. The SIS model is also based on the “control group” concept of shared management of policies, resources, and operations, a concept derived from the BJA Organized Crime Narcotics (OCN) Trafficking Enforcement Program. The OCN Program’s control group is a management mechanism whereby joint decisions are formulated on operational policies and on allocation and management of investigation and prosecution resources in multiagency narcotics enforcement efforts.

Project Selection Process

The agencies of state governments that were applicants for SIS Program funding were selected through a competitive process that included review by a peer panel comprised of criminal justice experts from outside the U.S. Department of Justice. The SIS Program began its individual project operations on October 1, 1993, with the selection of and funding awards to the Tennessee Bureau of Investigation and the Wisconsin Department of Justice as host agencies for their respective statewide intelligence system projects. On October 1, 1994, BJA awarded SIS Program funds to three additional agencies—the Connecticut State Police, the North Dakota Office of Attorney General, and the Utah Department of Public Safety.

Program Guidance

Program management and support were provided to the SIS projects through the Bureau of Justice Assistance, the RISS Program Guideline *Funding and Administration of the Regional Information Sharing Systems Program* (OJP G 3100.1A), and other technical advice and assistance rendered from the inception of the SIS Program. Federally funded SIS projects operated with support from the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended, and were also required to comply with the Criminal Intelligence Systems Operating Policies, 28 Code of Federal Regulations Part 23.

Upon initiation of the SIS Program, the Institute for Intergovernmental Research (IIR), a Florida nonprofit research organization, received a grant award from BJA to provide technical assistance and training support services to each SIS project site. IIR assisted the sites in activities such as developing formal intergovernmental agreements with participating agencies based on OCN Program concepts, designing and developing project intelligence database information systems, and selecting appropriate computer hardware and software compatible with the RISS Intelligence Centers. IIR also provided problem-specific technical assistance to each implementing agency as needs were identified and reported to BJA on the development and progress of the projects.

Structure of This Monograph

This report describes:

- The SIS Program and its goals, objectives, and components.
- SIS Program strategy and implementation actions.
- Implementation progress of each SIS project.
- Lessons learned from the development and implementation of the various statewide criminal intelligence systems.

The Appendixes include sample SIS project operating policies, procedures, and agreements.

The Statewide Intelligence Systems (SIS) Program

The SIS Program was established by the Bureau of Justice Assistance to develop and test a model criminal intelligence information-sharing system based on the design of the BJA-sponsored OCN Program's shared management strategy and compatible with information systems operated by RISS which is another BJA-sponsored program. The centerpiece of the OCN Program was a formal management control group that made joint decisions on operational policies and on allocation and management of investigation and prosecution resources. The SIS model intelligence-sharing system utilized the OCN control group concept to assist the lead agency in an SIS project in planning, organizing, and implementing the statewide intelligence system as well as in establishing policies for operating the system.

The SIS Program was designed to develop and test a model criminal intelligence information-sharing system.

The lack of coordination and exchange of information by both investigators and prosecutors—that is, the diffusion of responsibility among local, state, and federal law enforcement agencies—works to the advantage of organized criminal groups. Major criminal conspiracies span jurisdictional boundaries, requiring multiple agencies to successfully investigate and prosecute offenders. Individual law enforcement agencies often lack the capabilities to assemble or exchange intelligence about such criminal conspiracies, to centrally manage and effectively allocate their resources, or to coordinate their enforcement efforts. Also, they typically possess only a part of the legal authority necessary for a unified response to the criminal threat. Consequently, the reaction of the law enforcement community to major criminal offenses may be fragmented, limited, or even counterproductive.

Addressing the Crime Problem

Despite long-standing efforts by law enforcement agencies to overcome organized crime narcotics trafficking and gang violence, the enormous profits derived from these and other illicit criminal activities make their control the greatest challenge facing U.S. law enforcement today. Developing effective cases against high-echelon criminal conspirators requires the maximum utilization of investigative expertise, as well as innovative information collection techniques. Successful cases most often result when skilled local, state, and federal investigators and prosecutors pool their resources, capabilities, and expertise in planned and coordinated enforcement actions, and where there is free and efficient exchange of information and intelligence regarding criminal activities.

OCN and RISS Programs

In response to this assessment of multijurisdictional criminal conspiracies and the shortcomings of many law enforcement responses, in late 1986 the Bureau of Justice Assistance developed the OCN Program as a discretionary grant funding program. The goal of the OCN Program was to enhance, through shared management of resources and joint operational decisionmaking, the ability of local, state, and federal law enforcement agencies to remove specifically targeted major narcotics trafficking conspiracies and offenders through investigation, arrest, prosecution, and conviction.

The key aspects of the OCN Program strategy that were relevant to the SIS Program were the promotion of a multiagency enforcement response targeting major

criminal conspiracies operating across multiple jurisdictions, and the establishment of a formal mechanism whereby investigative resources targeting offenses and offenders could be allocated, focused, and managed on a shared basis. Critical to the success of the OCN Program was a shared management system to direct and administer the joint agency resources. Overall project direction was shared equally by the participating law enforcement agencies, and all decisions regarding operations and administration were required to be unanimous.

This OCN Program requirement accomplished several purposes. First, criteria were mutually established to identify, select, and prioritize investigative strategies. The resources and skills required to accomplish the joint activities were identified, acquired, and assigned throughout the duration of the effort. Finally, the OCN project established a management system to coordinate and monitor system activities to ensure proper timing of activities as well as to facilitate decisionmaking concerning investigative activity continuance, referral, redirection, or closure.

The SIS Program model intelligence-sharing system utilized the OCN Program's shared management concept to assist in planning, organizing, implementing, and operating the statewide intelligence systems. The SIS Program model was also compatible with the BJA-funded RISS Program, which supports state and local law enforcement investigation and prosecution efforts, especially in the area of sharing criminal intelligence information.

The SIS Program required funded projects to comply with provisions of the Criminal Intelligence Systems Operating Policies, 28 Code of Federal Regulations (CFR) Part 23, and prohibited them from adopting policies that conflict with principles of the RISS Program Guideline *Funding and Administration of the Regional Information Sharing Systems Program* (OJP G 3100.1A). Criminal intelligence data submissions to the SIS projects were also required to meet RISS Program requirements for information submission. Agencies participating in the SIS Program were required to identify other public state and local funds that would be dedicated to the effort.

Program Goals

The overall goal of the SIS Program was to demonstrate the effectiveness of shared management decisionmaking in the collection, storage, and dissemination of criminal intelligence information on a statewide basis. Specific goals of the SIS Program were to:

- Develop a statewide criminal intelligence-sharing model.
- Implement SIS projects in selected jurisdictions.
- Disseminate information for replication or development of effective statewide intelligence-sharing projects.

Program Objectives

The objectives of the SIS Program were to:

- Assess the applicability and adaptability of the OCN Program shared management concept to a statewide intelligence-sharing program.
- Develop a statewide intelligence-sharing model.
- Demonstrate the statewide intelligence-sharing model.
- Provide training and technical assistance to the SIS Program demonstration sites in development of a statewide intelligence-sharing model.
- Evaluate the SIS project demonstrations of intelligence-sharing models.
- Disseminate the results and promote program replication.

Administrative Components

Each SIS project was required to consist of a formally organized group of *participating* law enforcement agencies (one of which is the *applicant* or lead agency) and a project *control* (or oversight) *group*, described in more detail below.

Applicant Agency. The applicant or lead agency was a state agency that agreed to accept responsibility for preparation of the BJA grant application, for project administrative and fiscal matters as well as for

establishing policies and developing guidelines for the implementation and operation of the SIS. The applicant agency was the host for the computerized statewide criminal intelligence information-sharing system and was responsible for developing the necessary computer programs and systems to provide participating law enforcement agencies with system access capabilities.

Control Group. The SIS Program model was planned, organized, implemented, managed, and promoted by a control group consisting of, at a minimum, the SIS project applicant/host agency, a state law enforcement agency, and a local law enforcement agency. Applicants were encouraged to include the state attorney general's office, or other similar legal advisory agency, and additional local law enforcement agencies as control group members. A representative of the appropriate RISS Program Intelligence Center was required to be included as a nonvoting control group member.

Each SIS project control (or oversight) group was expected to assist the lead agency in establishing policies and developing guidelines for the implementation and operation of the SIS project. Members of the SIS control group were required to sign an agreement (or memorandum of understanding) to assist the lead agency in planning, organizing, implementing, managing, and promoting the SIS project. (Appendix C contains a sample memorandum of understanding.)

The SIS control group addressed issues such as:

- Eligibility of participating agencies.
- Information submission criteria.
- Information inquiry, access, and dissemination criteria.
- Information retention and deletion criteria.
- Security of information.
- Necessary audit trails.

Members of the control group had an equal vote in all matters raised before the group, and decisions of the control group were required to be unanimous. The head of the lead agency, or designee, served as chair of the SIS control group.

Participating Agencies. Each SIS project was composed of participating law enforcement agencies that included, at a minimum, the SIS project applicant/host agency, a state law enforcement agency, and a local law enforcement agency. Applicants often also included as participating agencies the state attorney general's office or other similar legal advisory agency, other state law enforcement agencies, additional local law enforcement agencies, and the appropriate RISS Program Intelligence Center.

The senior agency administrator of each participating agency was required to enter into an agreement with the head of the lead agency affirming his or her intention to fully participate in the SIS project by sharing criminal intelligence information in compliance with the policies and procedures promulgated

by the lead agency and the SIS control group and 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, where applicable. (Appendix D contains a sample participation agreement.)

Each SIS project consisted of *participating* law enforcement agencies (one of which is the *applicant* or lead agency) and a project *control* (or oversight) *group*.

Program Strategy and Implementation

.....

The following stages comprised the implementation strategy for the SIS projects:

Assessment

Each project conducted a review of the federal program guidelines for both the OCN and RISS Programs to ascertain the essential strategies and requirements that applied to the SIS project. An assessment was made of statewide and local criminal intelligence systems operating in the state, as well as the criminal intelligence needs of state and local law enforcement and prosecution agencies. Results of these assessments were incorporated into the design of the individual statewide intelligence systems.

Development

This stage involved design and configuration of the statewide intelligence system and the preparation of an implementation plan. The implementation plan defined major activities, timelines, and resource requirements.

Implementation

After successful completion of the program development stage, each SIS project began implementation of its system; some projects adopted as a goal the enhancement of currently existing systems. A description of the development and implementation status of each SIS project is contained in the next chapter.

As a part of SIS Program implementation, the following technical training, policy research assistance, coordination, and data collection activities were conducted by IIR:

- SIS project officials were assisted in addressing issues and administrative matters related to implementation of project control groups and development of their statewide intelligence systems.
- Software suitable for SIS demonstration sites, including RISSNET (the RISS Program intelligence database pointer system) and alternative software, was identified.
- Model operating policies and procedures for intelligence information-sharing systems were developed.
- Technical assistance was provided to SIS projects in project development, implementation, and refinement, including assisting projects involving system design and preparation of a program operations manual that described SIS policies, procedures, and practices.
- Assistance was provided to BJA to refine and modify the SIS Program model as necessary.
- Selected statewide intelligence systems not funded by the SIS Program were reviewed for compliance with 28 CFR Part 23, Criminal Intelligence Systems Operating Policies.
- Three SIS Program cluster conferences were conducted.
- Coordination and technical assistance were provided to support development of a version of the RISSNET database application for SIS project sites and other states interested in the SIS Program to facilitate ready hookup with the RISS Intelligence Centers.
- The continued development of RISSNET intelligence database software was coordinated with the RISS Intelligence Centers and system developers for use by the SIS projects.

- Documentation for the RISSNET intelligence database application, which included system manuals, data element descriptions, database table values, and functional specifications, was periodically provided to facilitate compatibility of SIS project databases with RISS Intelligence Center databases.
- Assistance was provided to the SIS projects regarding the design and functions of the RISSNET database application.
- Technical training and assistance were provided to SIS project representatives on 28 CFR Part 23 requirements.

Summary Descriptions of the SIS Projects

.....

This chapter contains summary descriptions of each of the five projects funded under the Bureau of Justice Assistance Statewide Intelligence Systems Program as well as a discussion of other intelligence systems which provided information through a national mail survey. Each of the agencies selected to participate in the SIS Program (with the exception of the Utah Department of Public Safety) conducted an assessment of law enforcement agencies in its state to determine which features and capabilities were desired in a statewide intelligence system. The Utah Department of Public Safety had already implemented a statewide intelligence system through the use of state funds combined with federal formula grant funds and used SIS Program funds to enhance and expand the existing Utah system. Each of these projects formed a control group to assist and advise in the implementation of the SIS and the setting of operational policies and procedures.

At the time this publication was drafted, the SIS projects in Tennessee, Wisconsin, North Dakota, and Connecticut were in various stages of development and implementation of their statewide intelligence systems. Utah had completed the enhancement and expansion of its system.

The following descriptions of the five SIS projects present and describe:

- Decisions that were made on the kind of system that would be implemented.
- A summary of progress in implementing the system selected.

- Control group member agencies.
- Grant award information.

Tennessee Bureau of Investigation SIS Project

Each host agency participating in the SIS Program conducted an assessment of the intelligence system features and capabilities needed by law enforcement in its state.

When officials from the Tennessee Bureau of Investigation (TBI) applied for SIS Program funding, the Tennessee Information Enforcement System (TIES) Network (the primary operational network serving all law enforcement agencies in Tennessee) and the Tennessee Crime Information System (TCIS) had been effectively interfaced for several years. Most of Tennessee's criminal intelligence databases were available through either TIES or TCIS.

After receiving the SIS funding award, TBI officials traveled to California to observe the California Statewide Integrated Narcotics System (SINS), which included an intelligence database application component called RISSNET. The SINS effort was being developed to provide for automated multiagency access to narcotics intelligence information. Tennessee officials concluded that the SINS and RISSNET component hardware platform was not compatible with the existing TBI computer equipment, nor would it be available in a timeframe that would meet their needs, so they explored other alternatives. After a review and assessment of Tennessee's SIS needs were completed, TBI SIS project officials determined that the most appropriate option would be for their system, the Automated Criminal Intelligence System of Tennessee (ACIST), to reside on the existing TCIS, which was located on an IBM 9370 computer.

A commercial database software package—Drug Track IV—was subsequently purchased for use on TBI’s existing IBM mainframe hardware. Although the name “Drug Track IV” suggests a narcotics information-based system, the software package offers broad intelligence gathering capabilities and modifiable software codes.

TBI SIS project officials also purchased and installed a local area network at TBI headquarters to integrate with the statewide system. The Drug Track IV software was installed and modified to serve as the Tennessee statewide intelligence database application. SIS project staff modified the Drug Track IV software by adding features needed for the statewide system and for compliance with 28 CFR Part 23. Security features such as encryption and decryption were also tested.

In late 1995, after problems and limitations in adapting the Drug Track IV program were encountered, a decision was made to undertake a complete rewrite of the software using a more current relational database software package that better suited the project’s needs. SIS project officials completed programming for the initial version of the intelligence database application in early 1996, and further enhancements were implemented in mid-1997. After testing the initial version in early 1996, SIS project staff began electronically connecting law enforcement agencies throughout the state, subsequently linking 248 agencies through the TIES Network. The staff used the existing law enforcement communications system operated by TBI as the backbone for the remote connections. Tennessee had approximately 10,000 officers in nearly 400 agencies that potentially could be connected to the statewide intelligence system. Tennessee SIS project officials also submitted a formal request for remote terminal access approval to the U.S. Department of Justice, Office of Justice Programs.

Portions of the TBI SIS award were used to complete the ACIST database and to research hardware and software solutions for the interface to Tennessee’s RISS

Intelligence Center (the Regional Organized Crime Information Center—ROCIC). The interface to be developed would be a model for electronically connecting ROCIC member agencies participating in ACIST to the RISSNET intelligence database application. Efforts to implement the interface from ACIST to ROCIC and RISSNET were delayed due to the subsequent development and implementation of Internet/intranet technology by the RISS Intelligence Centers, including ROCIC. The interface would instead be pursued through ongoing cooperative efforts between the TBI SIS project and ROCIC after SIS funding ended. The resultant Tennessee SIS system would be made available for replication by other agencies that wished to emulate the system.

Tennessee developed the Automated Criminal Intelligence System of Tennessee (ACIST), which is planned ultimately to connect nearly 400 agencies (with 10,000 officers).

Project Control Group Member Agencies

- Tennessee Attorney General
- Tennessee Bureau of Investigation
- Knoxville Police Department
- Regional Organized Crime Information Center (ROCIC) (RISS Intelligence Center)

Grant Award Information

Tennessee’s initial SIS grant included funds for four law enforcement information coordinator positions and two administrative secretary positions. The supplemental grant award did not include any funds for personnel.

Grant Period	Grant Award	Amount
10/01/93 – 12/31/95	Initial	\$365,000
10/01/95 – 12/31/96	Supplemental	\$100,000
01/01/97 – 06/30/97	Extension	No additional funds

Tennessee’s grant award for development of the statewide intelligence system ended June 30, 1997.

Wisconsin Department of Justice SIS Project

Pursuant to their SIS project grant award, Wisconsin Department of Justice (DOJ) officials initially conducted a review and assessment of other intelligence systems to evaluate whether Wisconsin would be able to implement or adopt a system that already had been developed. Three intelligence programs were identified and visited for evaluation: the Gulf States Intelligence Center in Alabama, the California SINS, and the Utah Law Enforcement Intelligence Network (ULEIN). The primary obstacle Wisconsin faced in trying to adopt any of these three programs was incompatibility of technical computer platforms; either the operating system database or the programming language of each of the three systems reviewed was found to be incompatible with the goal of Wisconsin DOJ officials to develop their state's system on a UNIX computer platform.

After additional review and assessment, Wisconsin SIS project officials decided to adopt the New Mexico Department of Public Safety intelligence system—NeMISIS—as Wisconsin's statewide system, which would be known as WisLEIN (Wisconsin Law Enforcement Intelligence Network). Wisconsin SIS project officials then contracted with the same company that had developed the New Mexico system to make modifications to that system for use in Wisconsin. WisLEIN was developed using Oracle software on a UNIX platform.

The software developed was initially installed by the Wisconsin SIS project staff as a demonstration version. SIS project staff then identified needed modifications to the Oracle software, which were subsequently provided by the contractor, installed, and tested. After testing and debugging of the modified system, Wisconsin SIS project staff began entering data and preparing to conduct a preliminary test of WisLEIN by initially connecting four agencies. Wisconsin SIS project

officials also submitted a formal request for remote terminal access approval to the U.S. Department of Justice, Office of Justice Programs.

Wisconsin SIS project staff planned to connect more than 160 agencies to the system by early 1998. Depending on funding availability, the system is ultimately to connect more than 300 agencies with approximately 10,000 Wisconsin law enforcement officers. SIS project officials also began upgrading their statewide communications network in order to make the intelligence system available to any law enforcement agency in the state through a dialup telephone connection. The WisLEIN system will be made available for replication by other agencies that wish to emulate the Wisconsin system.

Wisconsin developed the Wisconsin Law Enforcement Intelligence Network, (WisLEIN) which is ultimately to connect more than 300 agencies (with 10,000 officers).

Project Control Group Member Agencies

- Southeast: Milwaukee County Sheriff
- Southwest: Madison Police Department
- Northeast: Green Bay Police Department
- Northwest: Eau Claire County Sheriff

At-Large Representatives

- Wausau Police Department
- Wisconsin Department of Justice, Division of Narcotics Enforcement
- U.S. Attorney, Western District of Wisconsin

Ex Officio Members

- Division of Criminal Investigation, Wisconsin Department of Justice
- Wisconsin State Patrol
- U.S. Drug Enforcement Administration
- Federal Bureau of Investigation
- Mid-States Organized Crime Information Center (RISS Intelligence Center)

Grant Award Information

Wisconsin's initial grant award included funding for one systems analyst (half-time), one management information specialist, and four regional intelligence liaisons. The supplemental grants included funds for one management information specialist.

Grant Period	Grant Award	Amount
10/01/93 – 12/31/95	Initial	\$365,000
01/01/96 – 04/30/96	Extension	No additional funds
10/01/95 – 12/31/96	Supplemental	\$100,000

Wisconsin's grant award for development of the statewide intelligence system ended December 31, 1996.

Connecticut State Police SIS Project

Upon receipt of their SIS grant award, Connecticut State Police officials reviewed three other state intelligence information systems: New Mexico's NeMISIS, Utah's ULEIN, and Wisconsin's WisLEIN. However, state and department policies existed regarding preferred or mandated hardware, operating systems, and communications software and hardware that were required to be taken into consideration. For example, the Connecticut system was required to be designed to operate on the platform used by Connecticut's National Law Enforcement Telecommunications System—the Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) system.

The Connecticut SIS project was designed to receive significant amounts of data through electronic transfer and interface and established a goal that the system be as easy to operate and as economical as possible for its users. A direct link to Connecticut's COLLECT system was only available through Memorex/Telex machines. All of the above factors impacted the Connecticut SIS project decision to develop Connecticut's statewide intelligence system using a contractor.

Connecticut developed the Statewide Police Intelligence Network (SPIN), which is ultimately to connect the state's 7,457 law enforcement officers.

Subsequently, Connecticut's Criminal Justice Information System (CJIS) policy board approved funding for the development of a multiagency criminal justice information system. The Connecticut SIS project staff demonstrated their project's conceptual design to the CJIS policy board and related their intention to link with the approved criminal justice information system in the future.

Connecticut SIS project officials next finalized a request for proposals to obtain bids for developing the statewide intelligence system. The contract was awarded in 1996. Connecticut SIS project officials also submitted a formal request for remote terminal access approval to the U.S.

Department of Justice, Office of Justice Programs.

The following phased approach was planned to test and network the system:

Phase I: Scheduled for late 1996

10 remote sites serving 43 sworn officers

Phase II: Scheduled for mid-1997

18 remote sites serving 1,275 sworn officers

Phase III: Scheduled for late 1997

60 remote sites serving 6,200 sworn officers

The Connecticut SIS grant was approved by BJA for extension to March 31, 1998. Five agencies were involved in testing the beta version of the intelligence database referred to as the Statewide Police Intelligence Network (SPIN). Feedback from the test agencies was received and needed revisions were made to the database, which was developed using Lotus Notes. Some problems experienced by the test sites were in the area of communications and in the slow retrieval times from remote sites. The contractor subsequently completed the name entry and inquiry segments of the database.

By the end of 1997, Connecticut SIS project officials forecast that approximately 83 percent of their state's 7,457 law enforcement officers would have access to the system being implemented. However, delays in system testing and acceptance pushed completion of

later phases to 1998. In late 1997, 15 agencies were participating in system testing. The Connecticut SIS system would be made available for replication by other agencies that wished to emulate it.

Project Control Group Member Agencies

- Connecticut State Police, Connecticut Department of Public Safety
- Connecticut Department of Corrections
- Connecticut Office of Policy and Management
- States Attorney's Office
- State Narcotics Task Force
- Stamford Police Department
- Waterford Police Department
- Middletown Police Department
- Monroe Police Department
- Bridgeport Police Department
- Hartford Police Department
- New England State Police Information Network (RISS Intelligence Center)
- U.S. Attorney's Office
- U.S. Drug Enforcement Administration
- Federal Bureau of Investigation

North Dakota developed the North Dakota Law Enforcement Intelligence Network (LEIN), which is ultimately to connect 90 agencies (with 1,700 officers).

Grant Award Information

Connecticut's initial grant included funds for one data programmer analyst (part-time).

Grant Period	Grant Award	Amount
10/01/94 – 12/31/95	Initial	\$265,000
01/01/96 – 04/30/96	Extension	No additional funds
05/01/96 – 09/30/96	Extension	No additional funds
10/01/95 – 03/31/97	Supplemental	\$200,000
04/01/97 – 09/30/97	Extension	No additional funds
10/01/97 – 12/31/97	Extension	No additional funds
01/01/98 – 03/31/98	Extension	No additional funds

Connecticut's grant award for development of the statewide intelligence system was scheduled to end in early 1998.

North Dakota Office of Attorney General SIS Project

Upon receipt of the SIS project grant funding award, officials of the North Dakota Office of Attorney General collected and analyzed information describing intelligence systems from the Royal Canadian Mounted Police, Canadian Intelligence Service, and the states of South Dakota, Minnesota, Nebraska, Kansas,

Missouri, Iowa, Wisconsin, Illinois, and Utah. Because the North Dakota Bureau of Criminal Investigation had an existing automated intelligence system (IBM AS/400 system) for in-house use, representatives from North Dakota traveled to Salt Lake City, Utah, to review the Utah system, which was also developed on AS/400 hardware and software.

After reviewing Utah's Law Enforcement Intelligence Network, the North Dakota Office of Attorney General SIS project officials decided to adopt Utah's system specifications and features and to use their North Dakota SIS project staff to rewrite the software on a new IBM AS/400. The North Dakota SIS project staff used software development tools to implement a prototype system for their users to test and provide input for modifications and enhancements. North Dakota SIS project officials also submitted a formal request for remote terminal access approval to the U.S. Department of Justice, Office of Justice Programs.

The North Dakota SIS project, referred to as North Dakota's Law Enforcement Intelligence Network (LEIN), initially connected online all ten of North Dakota's drug task forces, which comprised 52 agencies. The system was then expanded by connecting eight local law enforcement agencies that were members of the SIS project control group (referred to as the Executive Committee). After these

agencies thoroughly tested the system, plans were to expand to additional agencies in the state to achieve a total of 90 law enforcement agencies serving approximately 1,700 law enforcement officers. At the time of this report, nearly 50 agencies were participating. The LEIN system will be made available for replication by other agencies that wish to emulate the North Dakota system.

Project Control Group Member Agencies (Executive Committee)

- North Dakota Bureau of Criminal Investigation
- Cavalier County Sheriff's Office
- Dickinson Police Department
- Mandan Police Department
- Minot Police Department
- Stutsman County Sheriff's Office
- Walsh County Sheriff's Office
- West Fargo Police Department
- Williams County Sheriff's Office
- Mid-States Organized Crime Information Center (RISS Intelligence Center)

Utah expanded and enhanced the existing Utah Law Enforcement Intelligence Network (ULEIN), which connects 220 agencies representing 97 percent of the state's law enforcement agencies.

Grant Award Information

North Dakota's initial grant included funds for one project coordinator/analyst, one computer programmer, and one administrative secretary.

Grant Period	Grant Award	Amount
10/01/94 – 12/31/95	Initial	\$265,000
01/01/96 – 06/30/96	Extension	No additional funds
07/01/96 – 07/31/96	Extension	No additional funds
10/01/95 – 03/31/97	Supplemental	\$200,000
04/01/97 – 06/30/97	Extension	No additional funds
07/01/97 – 12/31/97	Extension	No additional funds

North Dakota's grant award for development of the statewide intelligence system ended December 31, 1997.

Utah Department of Public Safety SIS Project

The Utah Department of Public Safety Division of Investigations and the Utah Department of Corrections separately had begun developing intelligence data programs as early as 1989. In 1990, each of these agencies determined it would be more cost-efficient and productive if they combined their resources and efforts in this area. They agreed that the Utah Department of Public Safety would act as the central coordinating and planning agency. A five-year plan was developed to centrally locate all data storage equipment and to begin integrating intelligence information between all federal, state, and local law enforcement agencies in Utah. The intelligence network was initiated by connecting 15 existing multijurisdictional task forces located throughout the state.

This was the first stage of what was to become ULEIN.

By 1991, Utah officials determined that their existing software would not meet the needs of the expanding system, and the process was begun to procure supplemental system funding. Additional funds were provided by the Utah State Legislature, along with state-managed BJA formula grant funds. The combined funds were used to purchase an IBM AS/400 mainframe computer in 1992. The initial database program that formally established ULEIN was then completed.

By 1994, ULEIN had grown from a simple network to an advanced system to store and process criminal intelligence data. More than 90 percent of Utah's law enforcement agencies were participating in ULEIN at that time. Because of the expansion of the system and the growth in the participation level, Utah SIS project officials requested and received a supplemental grant from BJA to purchase additional hardware and software

to enhance the state intelligence system to make communicating with systems of other agencies easier.

SIS project staff acquired and installed equipment upgrades that significantly improved the efficiency and operation of Utah's system. Additional software was also purchased to allow easier access to the system for more users at a lower cost and to install a "firewall" security device for the system. The firewall, when fully implemented, would allow access to the system through the Internet, abandoning the requirement for expensive, dedicated communication lines. In fact, because additional communication lines were not available, additional users could not be added to the system without the firewall security enhancement.

The ULEIN system eventually supported 220 local, state, and federal agencies, representing approximately 97 percent of Utah's law enforcement agencies. Utah's regional RISS Intelligence Center, the Rocky Mountain Information Network (RMIN), was also connected to the system, and the state was working on connecting the Utah system with state systems in Colorado and Wyoming by early 1998, as well as discussing connection with the state of North Dakota statewide intelligence system. The ULEIN system is available for replication by other agencies that wish to emulate the Utah system.

Control Group Member Agencies (Executive Board)

- Utah Division of Investigation
- Salt Lake City Police Department
- Salt Lake County Sheriff's Office
- Tooele County Sheriff's Office
- Utah County Sheriff's Office
- Ogden Police Department
- Utah Chiefs of Police Association
- Utah Sheriff's Association
- U.S. Attorney's Office
- U.S. Drug Enforcement Administration
- Federal Bureau of Investigation
- Internal Revenue Service
- U.S. Customs Service

Advisory Board

- Utah Department of Corrections
- Utah Office of State Attorney General
- Rocky Mountain Information Network (RISS Intelligence Center)
- Salt Lake County Law Enforcement Administrators
- Statewide Association of Prosecutors
- Utah County Law Enforcement Administrators
- Weber/Morgan Law Enforcement Administrators

Grant Award Information

Utah's grant was for equipment enhancements only.

Grant Period	Grant Award	Amount
10/01/94 – 09/30/95	Supplemental	\$100,000
10/01/95 – 12/31/95	Extension	

Utah's grant award for enhancement of the statewide intelligence system ended December 31, 1995.

Other Systems

During late 1996, IIR conducted a survey of state criminal intelligence information systems to collect current information on the status of state intelligence systems across the United States. The survey was distributed to state agencies across the country by the RISS Intelligence Centers. In addition to agency demographic information, the following types of information were gathered:

- The state's current and planned criminal intelligence information databases.
- The means of access to information stored in the databases.
- The number of current statewide criminal intelligence systems.
- The agencies hosting the various intelligence systems.
- Intelligence system computer hardware, software, and funding sources.
- Intelligence system compliance with 28 CFR Part 23.

- The type of criminal activity information in the databases.
- Whether or not the intelligence system included implementation of the following:
 - written system procedures and policies
 - formal agreements to comply with system policies
 - system security procedures
 - system control (oversight) groups
 - Internet access

Results of the survey are presented in the next chapter.

Lessons Learned

.....

The SIS Program was established to test the theory that a criminal intelligence-sharing model that uses shared management decisionmaking in the collection, storage, and dissemination of intelligence information on a statewide basis will be operationally effective, efficient, and useful. Many states had, in the past, implemented systems for gathering, storing, and disseminating criminal intelligence information on a statewide basis—information systems that varied greatly in configuration, complexity, focus, and management. The SIS Program model was approved for implementation and examination by BJA to assess whether a system of its design was in fact effective.

The experiences described here result from the initiation, development, and implementation of the SIS Program. The Program received its initial funding in 1993 from BJA. By early 1998, federal funding for the SIS Program for all of the five SIS project sites was scheduled to end. Program results to date offer support for the theory that a statewide criminal intelligence-sharing model that maximizes the effectiveness of shared management decisionmaking in the collection, storage, and dissemination of criminal intelligence information on a statewide basis is an effective model. This chapter describes some of the lessons learned from the implementation and operation of the statewide intelligence-sharing system projects.

This monograph was prepared to assist state and local law enforcement and criminal justice agencies that are interested in joining forces and sharing resources to combat multijurisdictional criminal activity through establishment of multijurisdictional intelligence systems. The monograph describes the steps necessary to successfully develop and implement a unique law enforcement criminal intelligence system—the model developed through the SIS Program. The information presented here should be useful to agencies conducting

a wide range of multijurisdictional law enforcement intelligence-sharing efforts. Policies and procedures for establishing and governing operation of intelligence systems, the types of developmental problems encountered, and the solutions attained are also presented.

The SIS Program intelligence-sharing system model was developed and designed for compatibility with the Regional Information Sharing Systems (RISS) Program, which is also funded by BJA. The RISS Program supports the exchange of criminal intelligence information among local, state, and federal law enforcement agencies. The SIS Program model was also based on the “control group” concept of shared management of policies, resources, and operations. This concept was derived from the OCN Program’s formal management control group that formulated joint decisions on operational policies and on allocation and management of investigation and prosecution resources in multiagency narcotics enforcement efforts. The SIS Program model intelligence-sharing system employed the OCN control group concept to assist the lead agency in an SIS project in planning, organizing, and implementing the statewide intelligence system and establishing policies for operating the system.

The SIS Program has thus far demonstrated the effectiveness of shared management decisionmaking in the collection, storage, and dissemination of criminal intelligence information on a statewide basis. The SIS Program:

- Assessed the applicability of the OCN Program’s shared management system and its adaptation to a statewide intelligence-sharing program.
- Developed a statewide intelligence-sharing model.
- Demonstrated the statewide intelligence sharing model.

- Provided training and technical assistance to the demonstration sites.
- Evaluated the SIS project demonstrations.
- Disseminated the results to promote program replication.

As improvements and modifications were made to the various statewide intelligence-sharing system projects participating in the SIS Program over their period of operation, the details were shared among the other SIS projects during periodic national SIS Program cluster conferences, and through regular site visits by program officials and project technical training and policy research assistance staff.

The first lesson learned from the program experience related to the concept of establishing and recommending one “model” system. The existence of various types of state computer systems (typically referred to as legacy systems) must be considered when implementing new or enhanced statewide intelligence-sharing systems. Use of industry standard applications and open systems architecture significantly facilitates the adaptation and modernization of legacy systems. The strengths of existing systems should be stressed while enhancing their value with open standards to provide easy access. This type of integration effort provides a highly efficient use of resources by taking advantage of systems already in place. Rather than recommend one specific set of system hardware and software requirements, the various SIS Program projects worked with their existing state systems and requirements and developed a number of computer system configurations that met the overall management and coordination principles of the SIS Program model. Implementation of the various statewide intelligence-sharing system projects resulted in the development of several systems which, although varying in some aspects, successfully applied the core concepts of the SIS model.

Thus, a single, comprehensive model did not result from program implementation experience, as originally anticipated. Substantial financial investments in computer systems already in place (other than intelligence systems) by the individual SIS Program state agencies dictated the computer platform chosen by each

state to ensure compatibility at minimal cost. Although the five systems were developed on different computer platforms, this actually benefited replication efforts by other agencies by demonstrating a wider range of systems and computer platforms that can be implemented to create SIS computer systems.

The Control Group

Perhaps the most unique feature of the SIS Program model was the control group decisionmaking and oversight processes. In a traditional multiagency organization, a “lead agency,” usually reporting to a board of directors, is designated. Designation of a lead agency sometimes results in serious friction or reduces the involvement of other participants to merely contributing resources to the lead agency and having little impact on management or operational activities. In such an arrangement, the board of directors, usually comprised of the administrators of the participating agencies, is often limited to establishing broad policies and strategies. The board is often chaired by the lead agency, which usually appoints the multiagency operational commander as well.

The SIS project control group was required to consist of, at minimum, the SIS project applicant/host agency, a state law enforcement agency, and a local law enforcement agency. Applicants were encouraged to include the state attorney general’s office or other legal agency and additional local law enforcement agencies as control group members. A representative of the appropriate RISS Intelligence Center was required to be included as a nonvoting control group member.

Management and operational decisionmaking were shared among agencies participating in the SIS project control group. The control group not only served as a governing board that made policy, but it also allocated project resources and jointly monitored SIS activities. Members of the SIS control group had equal votes on all project matters, and all control group decisions were required to be unanimous. Day-to-day supervision of project activities, once approved by the control group, often rested with the individual lead agency that applied for SIS funding and agreed to be the system administrator.

One of the first organizational tasks of a SIS project was determining the composition of the control group. Control groups varied from a minimum of four agencies to a maximum of 20. Some of the larger groups created ex officio members, executive committees or boards, or advisory board components to facilitate activities. The inclusion of a large number of agencies on a control group sometimes made decisionmaking more cumbersome and increased the logistical obstacles to scheduling meetings.

One of the initial problems faced by a SIS control group pertained to the agency designee who represented an agency in the group. Because many agencies had participated in previous cooperative, multijurisdictional efforts, including membership on task force boards of directors, there was sometimes a tendency to nominate the agency's chief executive to attend control group meetings. Over time it became apparent that agency chief executives were usually too busy, too involved in extradepartmental business, or too far out of the system's operational process to be the most effective choice for the control group representative.

Generally, it was found that the agency representative on the control group should be a system or operational commander or staff person, albeit one with direct access to the highest command levels of the parent agency. The control group representatives should be in the mainstream of the intelligence system operations of their own agencies so that they need little updating on ongoing project activities in which their agencies have the lead. The representatives should be able to commit their agencies' resources to a project without further approval and not be simply a message carrier.

SIS program guidelines intentionally offered no detailed advice on control group meeting format, frequency, or location. In all cases, these formalities were decided early in the project start-up process and modified over time. Most control groups met frequently, at least monthly, in the early stages of project implementation. Some maintained that frequency throughout the project period, but most groups met less frequently with the passage of time, and some control groups met only once each quarter.

Other Program Experience

Several other findings regarding SIS Program implementation and operation were observed:

- It was critical to SIS Program success that a state system become established and operational as soon as practicable.
- SIS projects with large control groups sometimes found it difficult to achieve unanimous decisions, which caused unnecessary delays.
- All SIS projects felt the control group concept was essential to adequately address policy oversight matters, but some experienced occasional difficulty in achieving unanimous decisions.
- One SIS project encountered a contractor that was late in delivering revised software, and a number of software items were delivered incomplete, incorrect, or not thoroughly tested prior to release.
- Another SIS project faced obstacles from policies established by its state officials that did not allow changes to the infrastructure of its data processing system to develop and implement the statewide intelligence system.
- Some SIS project participants suggested that the BJA program announcement and application process should have been simplified and set out more clearly what was to be accomplished.
- Some SIS projects suggested that grant reporting requirements should have been more clearly defined, and special conditions to the awards should have been more pertinent and specific to the projects.

Survey

In late 1996, IIR conducted a survey of state criminal intelligence information systems. The purpose of the survey was to collect current information on the status of state intelligence-sharing systems across the United States. The survey was distributed to state agencies across the country by the RISS Intelligence Centers. Fifty-four surveys were returned (some states submitted more than one). Information from SIS project states was added to the survey results, resulting in a compilation of agencies representing 41 separate states.

Following is a summary of the information obtained from the survey:

- Thirty-four state agencies had criminal intelligence information databases in operation; six did not.
- Twenty-eight agencies operated databases as statewide criminal intelligence information systems for the exchange of information with participating law enforcement agencies throughout the state; eight did not.
- Twenty-six agencies responded that a total of 3,062 agencies in their states participated in the statewide systems. Responses ranged from zero to 500 agencies, with an average system size of 118 agencies.
- Thirty-three responding agencies indicated they were the host agency for maintaining and operating the state system.
- One-third (14) of the 41 states indicated their systems operated with federal funding support, while two-thirds (27) indicated they operated only with state funds.
- Nearly 90 percent (39) of the agencies indicated their database/system operated in compliance with the provisions of 28 CFR Part 23 (Criminal Intelligence Systems Operating Policies), while five agencies did not know. None of the respondents indicated their system was not in compliance.
- Half the agencies (23) indicated they had a control group or policy board to assist their agency in developing and implementing policies for operation of the criminal intelligence database/system, while half (22) did not.
- Two-thirds of the agencies indicated that criminal intelligence personnel in their agencies had access to the Internet, while one-third (14) did not.
- In addition to the 34 agencies that were already operating a criminal intelligence database, six were in the process of developing a criminal intelligence information database, and three more had plans to develop a statewide intelligence system for use by law enforcement and/or criminal justice agencies in their state. Only one agency indicated it had no plans to develop a system.

SIS Program funding from BJA supported development of much needed criminal intelligence networks for exchange of criminal information among law enforcement agencies.

Conclusions

SIS Program funding from BJA supported the development of much needed criminal intelligence networks for exchange of information among law enforcement agencies to combat criminal activity. Successful implementation of the SIS projects provided for rapid access and online retrieval of information on narcotics trafficking, gangs, violent crime, and organized criminal groups by participating law enforcement agencies in each of the demonstration states.

The survey conducted in conjunction with the SIS Program disclosed that at least 43 state agencies operated criminal intelligence databases or were in the planning or development process for such systems. Most operated the databases as statewide criminal intelligence information systems for the exchange of information with participating law enforcement agencies throughout the state. A significant number of the states indicated their systems operated with federal funding support, and the overwhelming majority acknowledged the existence of federal criminal intelligence systems operating policies and their compliance with those regulations. Half of the states used control groups or policy boards to assist their agencies in developing and implementing policies for operation of the criminal intelligence database/systems.

The survey affirmed the significance of SIS Program concepts regarding the need for state intelligence systems, the development of improved methods to operate such systems, the potential federal role in developing recommended operational procedures and standards for such systems, the use of shared management decisionmaking in system operation, and the need for training and technical assistance in many of these areas.

When fully implemented, the five SIS projects have the potential to serve nearly 1,000 agencies and approximately 32,000 local (municipal and county), state, and federal law enforcement officers in the participating states. All of the statewide intelligence databases interfaced with the RISS Intelligence Center

in their respective geographical region to further expand the benefits to law enforcement agencies in rapid retrieval and exchange of criminal intelligence information. The RISS Intelligence Centers serve nearly 5,000 agencies comprised of over 576,000 law enforcement officers in all 50 states.

Appendixes



Appendix A

Statewide Intelligence System Sample Operating Policies And Procedures

Mission Statement

To provide a Statewide Intelligence System (SIS) for the timely sharing of criminal intelligence information among law enforcement and criminal justice agency personnel in an effort to prevent and control crime and in conformance with the privacy and constitutional rights of individuals.

Goals

Provide liaison, coordination, and resource assistance in the collection, storage, exchange or dissemination, and analysis of criminal intelligence information in ongoing multijurisdictional investigations or prosecution activities relating to specific areas of criminal activity (see Definitions).

Provide criminal intelligence information to law enforcement and criminal justice agency personnel on individuals and organizations involved in identified criminal organizations and enterprises.

Provide analysis of organized crime and criminal enterprises in [STATE]. This includes identification and/or projection of major changes in crime trends that may require adjustments in resource allocation.

General Operating Policies

Applicability

Federally funded criminal intelligence systems operating funding under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended, are required to comply with the U.S. Department of Justice (DOJ) Criminal Intelligence Systems Operating Policies, 28 CFR Part 23 (hereinafter referred to as 28 CFR Part 23—see copy attached as Appendix B). These Sample Operating Policies and Procedures incorporate the 28 CFR Part 23 requirements.

Coordination and Control

By authority of [STATE LAW], the [HEAD] of the [NAME OF LEAD AGENCY] (hereinafter referred to as Lead Agency) or an individual with general policymaking authority who has been expressly delegated by the [HEAD] of the Lead Agency shall be responsible for coordinating the SIS and ensuring that information in the SIS is maintained and transmitted in accordance with the standards set forth in these operating policies and procedures.

SIS Control Group

An SIS Control Group (or Oversight Board) shall be formed to assist the [NAME OF LEAD AGENCY] in establishing policies and developing guidelines for the implementation and operation of the SIS. The SIS Control Group shall also assist the Lead Agency with planning, organizing, managing, and promoting the SIS project. The SIS Control Group members shall be selected from or appointed by a Participating Agency and shall be required to enter into an agreement (see Statewide Intelligence System Control Group Sample Memorandum of Understanding attached as Appendix C) with the [HEAD] of the Lead Agency.

Participation

Participation in the SIS is open to federal, state, county, and local agencies with law enforcement or criminal investigative authority in [STATE].

Agencies participating in the SIS are required to sign a Participation Agreement (see sample copy attached as Appendix D) agreeing to follow the SIS operating policies and comply with 28 CFR Part 23.

The chief executive of each Participating Agency shall designate in writing one or more persons from among the bona fide employees of the Participating Agency to represent the Participating Agency in the SIS. These representatives will be referred to as “Access Officers.” The chief executive shall designate one Access Officer as the “Primary Representative.” The chief executive may also designate an “Alternate Representative” from among the Access Officers. Both the Primary and Alternate Representatives may remain Access Officers.

The chief executive of the Participating Agency may from time to time change or make new designations and may designate himself/herself as Primary Representative, Alternate Representative, or Access Officer.

Any change in the designation of the Primary Representative shall be in writing from the chief executive of the Participating Agency to the [HEAD] of the Lead Agency. Changes in the Alternate Representative or the Access Officer may be made by written notice from the Primary Representative unless the chief executive of the Participating Agency chooses to reserve that right.

The Primary Representative of the Participating Agency shall be the primary point of contact between the SIS Lead Agency central staff on administrative matters, and shall monitor agency compliance with the operating principles set forth in these operating policies and procedures.

Participating Agency Access Officers shall attend periodic SIS training and coordination sessions.

Criminal Activity Focus

Criminal intelligence information on individuals and organizations submitted to the SIS shall refer to significant multijurisdictional criminal activities. Some examples of criminal activity categories are:

- Narcotics manufacturing and/or trafficking
- Unlawful gambling
- Loan sharking
- Extortion
- Smuggling
- Vice and pornography
- Infiltration of legitimate businesses for illegitimate purposes

- Stolen securities
- Bribery
- Major crime including homicide, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, forgery, fencing stolen property, and arson
- Manufacture, use, or possession of explosive devices for fraud, intimidation, or political reasons
- Organized crime (see Definitions)
- Corruption of public officials
- Threats to public officials and private citizens
- Traveling criminals (see Definitions)
- Other designated multijurisdictional criminal activities

Operating Procedures

Information Storage and Retrieval System

The [STATE] SIS resides on a host computer system in the [NAME OF LEAD AGENCY] located at [ADDRESS OF THE LEAD AGENCY]. All information contained in the SIS shall be considered the property of the submitting agency and shall not be accessed or disseminated except as provided in these operating policies and procedures.

Submission of Information

All submissions of criminal intelligence information on individuals and organizations to the SIS are the property of the submitting agency.

Information may be submitted in either of two ways:

1. **Direct Entry:** Information may be entered directly from personal computer terminals that are linked by dedicated lines to the [NAME OF LEAD AGENCY] host computer. Screen-handling software and security measures will reside on the personal computer; however, data files and additional security measures will reside on the host computer system
2. **Indirect Entry:** If an agency does not have an access terminal, information may be submitted on approved forms or in format for entry by SIS-designated personnel. Information can be submitted in person, via telephone, mail, e-mail, or facsimile. Information submission shall be validated by an Access Officer or other designated agency personnel at the time of entry or submission to determine that the submitted information meets the criteria necessary for inclusion in the SIS.

Information Submission Criteria

The Lead Agency shall only collect and maintain criminal intelligence information concerning an individual if there is “reasonable suspicion” that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

The Lead Agency shall not collect or maintain criminal intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization, unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

Reasonable suspicion or “criminal predicate” is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. The Lead Agency is responsible for establishing the existence of reasonable suspicion of criminal activity, either through examination of supporting information submitted by a Participating Agency or by delegation of this responsibility to properly trained Participating Agency personnel which is subject to routine inspection and audit procedures established by the Lead Agency.

The Lead Agency shall not include in the SIS any information that has been obtained in violation of any applicable federal, state, or local law or ordinance. The Lead Agency is responsible for establishing that no information is entered in the SIS in violation of federal, state, or local laws, either through examination of supporting information submitted by a Participating Agency or by delegation of this responsibility to properly trained Participating Agency personnel which is subject to routine inspection and audit procedures established by the Lead Agency. Additionally, the subject should be identified by unique identifying characteristics, including but not limited to:

- Full Name
- Address
- Aliases
- Monikers
- Date of Birth
- Place of Birth
- Citizenship (if Alien, Identification Number)
- Social Security Number
- Driver’s License Number
- Physical Description: Height, Weight, Eye and Hair Color
- Violence Potential
- Distinguishing Scars, Marks, or Tattoos
- Criminal Identification Number
- Criminal Activity and/or Offenses
- Modus Operandi (see Definitions)
- Criminal Associates

Information submission criteria should also include the following:

- Date of Submittal of Information
- Name of Submitting Agency
- Submitting Officer’s Name

Labeling of Information

Information to be retained in the SIS shall be labeled for source reliability and content validity prior to entry or submission.

Source Reliability

The reliability of the source is an index of the consistency of the information the source provides.

The source shall be evaluated according to the following:

- **RELIABLE**—The reliability of the source is unquestioned or has been well tested in the past.
- **USUALLY RELIABLE**—The reliability of the source can usually be relied upon. The majority of the information provided in the past has proved to be reliable.
- **UNRELIABLE**—The reliability of the source has been sporadic in the past.
- **UNKNOWN**—The reliability of the source cannot be judged; authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity

The validity of information is an index of the accuracy or truth of the information. The validity of the information shall be assessed as follows:

- CONFIRMED—The information has been corroborated by an investigator or another reliable independent source.
- PROBABLE—The information is consistent with past accounts.
- DOUBTFUL—The information is inconsistent with past accounts.
- CANNOT BE JUDGED—The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

Information maintained in the SIS may be labeled using any combination of the above Source Reliability and Content Validity designations, *except* for the combination of “Unknown” for Source Reliability and “Cannot Be Judged” for Content Validity—this particular combination does not meet reasonable suspicion criteria.

Dissemination Level

The dissemination level is the classification of information and how it is to be shared with other Participating Agencies, if at all. If more than one agency submits information on the same subject and the information is linked in the automated database, the dissemination level viewed in the system must reflect the most restrictive dissemination level. Examples of levels of dissemination of information are:

- OPEN (All Information Released)—All information maintained in the system may be released to the inquiring party. No restrictions of dissemination are applied.
- RELEASE AGENCY NAME ONLY—Only the contributing Agency Name, Unit, Contact, and Contact Phone Number are released. No detailed information on the subject of the inquiry is released. The inquiring agency may contact the submitting agency for detailed information.
- RESTRICTED (No Information Released)—“Hits” or potential “hits” are NOT released. Access to information is restricted and, unless the inquiring party is the contributor of the information, the information may only be viewed by designated Lead Agency personnel. The contributing agency is notified of the “hit” either electronically or by telephone. The contributing agency has the option of whether or not to contact the inquiring agency.

Access Rights

Restrictions on release of the information based on the designated dissemination level are always enforced in the agency inquiry environment with the exception that a contributor of information may view the data he or she submitted regardless of the designated dissemination level.

For system administration and maintenance purposes, designated Lead Agency personnel may have access to all information regardless of the dissemination level.

Participating Agencies have access to any information they submit to the SIS and are responsible for the content, validity, and usefulness. The Primary Representative determines who within the Participating Agency has a need to access the agency’s records and to what extent. For example, clerks may be limited to data entry and may not be able to perform queries.

Telephone, e-mail, and facsimile requests for criminal intelligence information will be addressed only after the requester’s authorization is determined. If online electronic access is allowed, confirmation may be through use of passwords or other security devices.

Inquiry Procedures

Inquiries can be made without reasonable suspicion of criminal activity; however, for information to be placed in the SIS, reasonable suspicion must be established. [Note: A more restrictive policy may be adopted requiring that reasonable suspicion of criminal activity be established prior to making an inquiry.]

Any authorized Participating Agency employee may initiate an inquiry to the SIS, but information will be disseminated only to designated personnel [such as the Primary Access Officer or Alternate Access Officer] who have authorized access.

Prior to dissemination of information, the identity of the inquiring Access Officer must be confirmed. If online electronic access is allowed, confirmation may be through use of passwords or other security devices.

If access is by telephone, mail, e-mail, or facsimile, the Lead Agency may use a personal data sheet or security control card maintained on file. In this instance, release of information shall be made on a call-back basis only after verification of the identity of the Access Officer.

Dissemination of Information Procedures

The Lead Agency or authorized recipient shall disseminate criminal intelligence information only where there is a need-to-know and a right-to-know the information in the performance of a law enforcement activity.

The Lead Agency shall disseminate criminal intelligence information only to law enforcement or criminal investigative authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with these operating policies and procedures. CAVEAT: This paragraph shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

Dissemination Record

An audit trail or dissemination record is required when information is disseminated from the database. The record shall contain the following information:

- The date of dissemination of the information
- The name of the individual requesting the information
- The name of the agency requesting the information
- The reason for the release of the information (need-to-know/right-to-know)
- The information provided to the requester
- The name of the SIS staff member disseminating the information

This record can be created automatically by the database, or policies and procedures can be implemented to handle the audit trail/dissemination record manually.

Review and Purge Procedures

Reviewing and purging information in the SIS should be done on an ongoing basis. The maximum retention period is five years. [NOTE: Policies can be adopted for a retention period of less than five years.] If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period. The submitting agency may update and/or validate the submission and extend the retention period at any time. Updated or new

criminal activity from any Participating Agency may be used to extend the retention period if the original submitting agency is contacted and agrees.

The review, validation, and purge process may be a manual process, or an automated process, or a combination of both. A data field is required so that a determination can be made of how long the information has been in the SIS and when it is due for purging. Purge dates are initially calculated based on the submittal date and the submittal type and can be generated automatically, or the purge date could be manually entered. If a purge date is modified, then all links to the records must be evaluated and modified appropriately.

Procedures for Purge of Information

The Lead Agency may adopt a policy to purge information without notification to the submitting agency or adopt a policy to notify the submitting agency prior to purge of information to provide the submitting agency an opportunity to validate the submission and extend the retention period. The process adopted should not delay purge of information that has reached the end of its retention period; i.e., information may not remain in the database longer than the retention period without validation and updating.

Purge Without Notification to Submitting Agency

The Lead Agency should inform all Participating Agencies of the policy to purge information without notification. It is then incumbent on the submitting agency to track their submissions. If there has been no update or resubmission of the information by the submitting agency, then it is automatically purged at the end of the five-year period.

Notification Prior to Purge

The information can be returned to the submitting agency prior to the end of the established purge period with a request to resubmit the information.

Once a month the Primary Representative for each Participating Agency will be provided with a list of their submissions scheduled to be purged within the next 90 days. If the Participating Agency chooses to retain a submission, it must be validated by an Access Officer. Failure to review and validate the submission will result in the submission being purged at the end of a five-year period [or shorter period established by the Lead Agency].

The Access Officer conducting the review shall make a determination that some or all of the information contained in the submission continues to comply with 28 CFR Part 23 requirements. Information concerning each individual, group, association, corporation, business, or partnership named in the submission shall be reviewed to determine if that individual, group, association, corporation, business, or partnership continues to be reasonably suspected of being involved in the criminal activity described in the submission. If this determination is made, the Access Officer will notify the Lead Agency and the retention period will be extended. All information retained as a result of this review shall reflect the name of the reviewer, date of review, and explanation of decision to retain.

If this cannot be established, the name of the individual, group, association, corporation, business, or partnership will be deleted from the database.

The decision to purge information should be guided by the following considerations:

- The number of requests for the file/individual
- The validity of the data
- The reliability of the data

- Federal/state law
- The time in the file
- Present or future strategic or tactical intelligence utility
- Continuing compliance with 28 CFR Part 23 reasonable suspicion criteria and investigative interest of the submitting agency

Any information that is found to be misleading, obsolete, or otherwise unreliable will be purged on an ongoing basis by the Lead Agency and recipient agencies advised of such changes.

Destruction of Information

Material purged from the SIS will be returned to the submitting agency or confidentially destroyed. Only an administrative record of the purge will be maintained. No record of the names of individuals, organizations, etc., that are purged will be maintained by the Lead Agency.

Inspection and Audit of Files

The Lead Agency will periodically conduct audits and inspections of Participating Agency records that support submissions to the SIS database and compliance with operating principles set forth in 28 CFR Section 23.20 with regard to submissions made to the SIS.

The audits and inspections of Participating Agency files will be conducted randomly by a representative of the Lead Agency and are designed to review backup information to ensure continuing compliance with 28 CFR Part 23 is maintained by the submitting agency. A random number of Participating Agencies and a random number of submissions from those agencies will be selected for audit and inspection. The audit and inspection may be conducted onsite at the participating agency or through a mail process requiring certification of continuing compliance by the head of the agency.

Agencies participating in the SIS are not required to, but may, maintain files that support submissions to the SIS and that support compliance with these SIS operating policies and procedures (which incorporate compliance with 28 CFR Part 23) separately from other agency files. Inspection and audit of Participating Agency files will be conducted in such a manner so as to protect the confidentiality and sensitivity of Participating Agency intelligence records.

Security of SIS Files

In order to maintain the confidentiality of stored criminal intelligence information and to ensure the protection of the individual's right to privacy, the [Head] of the Lead Agency, or designee, shall be responsible for implementing the following security requirements for the SIS:

- The SIS database, manual or electronic, shall be located in a physically secured area that is restricted to designated authorized personnel.
- Only designated authorized personnel will have access to information stored in the SIS database.
- All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility and physical location housing the SIS database.
- All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- All hardcopy submissions and/or manual files will be secured by Lead Agency designated authorized personnel when not being used and at the end of each shift.

- Employment policies and procedures for screening/rejecting, transferring, or removing personnel having direct access to the SIS will be adopted.
- When direct remote terminal access is authorized by participating agencies, policies and procedures addressing the following additional security measures shall be adopted:
 - Identification of authorized remote terminals and security of terminals
 - Identification and verification of authorized access officer (remote terminal operator)
 - Levels of dissemination of information as directed by the submitting agency
 - Rejection of submissions unless critical data fields are completed
 - Technological safeguards on SIS access, use, dissemination, and review and purge
 - Physical security of the SIS
 - Training and certification of SIS Participating Agency personnel
 - Audits and inspections of SIS Participating Agencies, including: file data supporting submissions to the SIS, security of access terminals, and policy and procedure compliance
 - Documentation for audit trails of the entire SIS operation

Definitions

For the purposes of these operating policies and procedures:

- “Criminal activity”** is defined as any activity which violates state statutes, ordinances, or codes, and constitutes a criminal act under the law (excluding traffic violations).
- “Criminal associate”** is defined as an individual who is suspected of maintaining criminal associations and involvement with any individual, group, or organization reasonably suspected of engaging in criminal activity.
- “Criminal intelligence information”** is defined as data which has been evaluated to determine that it (1) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity; and (2) meets SIS submission criteria.
- “Criminal intelligence system”** or **“intelligence system”** is defined as the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.
- “Jurisdictional boundaries”** are defined as the area within any city, village, township, or county within the area served by the SIS.
- “Lead Agency”** is defined as the organization that operates a statewide intelligence system on behalf of a group of Participating Agencies.
- “Modus Operandi”** is defined as a unique method of operation for a specific type of crime and may not be immediately linked to an identifiable suspect.
- “Multijurisdictional”** criminal activity is defined as criminal activity that crosses jurisdictional lines and involves two or more separate and distinct jurisdictions.
- “Need-to-know”** is defined as the necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement or criminal justice authority.
- “Organized crime”** is defined as any organized group that has its leadership insulated from direct involvement in criminal acts and ensures organizational integrity in the event of a loss of leadership.
- “Participating Agency”** is defined as an agency of local, county, state, federal or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through a Statewide Intelligence System. A Participating Agency may be a member or a nonmember of a Statewide Intelligence System.
- “Reasonable suspicion”** or **“criminal predicate”** is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.
- “Right-to-know”** is defined as the legal authority to obtain or receive criminal intelligence information pursuant to court order, statute, or decisional law.
- “Statewide Intelligence System”** is defined as an intelligence system or criminal intelligence system that involves two or more agencies representing different governmental units or jurisdictions.
- “Traveling criminals”** is defined as individuals, groups, or organizations engaged in or otherwise associated with criminal activity that traverses jurisdictional boundaries.

Appendix B

Criminal Intelligence Systems Operating Policies 28 CFR Part 23

PART 23 — CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

- 23.1 Purpose.
 - 23.2 Background.
 - 23.3 Applicability.
 - 23.20 Operating principles.
 - 23.30 Funding guidelines.
 - 23.40 Monitoring and auditing of grants for the funding of intelligence systems.
- Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for federally funded projects are required.

§ 23.3 Applicability.

- (a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).
- (b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or

jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

- (a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.
- (b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.
- (c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
- (d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
- (e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.
- (f)
 - (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.
 - (2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.
- (g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the

information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

- (1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;
 - (2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;
 - (3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;
 - (4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;
 - (5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and
 - (6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.
- (h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.
- (i) If funds awarded under the Act are used to support the operation of an intelligence system, then:
- (1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and
 - (2) A project shall undertake no major modifications to system design without prior grantor agency approval.
- (j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.
- (k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

- (l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.
- (m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.
- (n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.
- (o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

- (a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.
- (b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:
 - (1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and
 - (2) Involve a significant degree of permanent criminal organization; or
 - (3) Are not limited to one jurisdiction.
- (c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.
- (d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:
 - (1) assume official responsibility and accountability for actions taken in the name of the joint entity, and
 - (2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance

with the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

- (e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

- (a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.
- (b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.
- (c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Appendix C

Statewide Intelligence System Control Group Sample Memorandum of Understanding

This Memorandum of Understanding (MOU) is entered into between the [HEAD] of the [NAME OF LEAD AGENCY] and the members of the Statewide Intelligence System (SIS) Control Group to govern the formation, participation, and related cooperation of the members of the SIS Control Group.

Objectives

The overall objective of the SIS Control Group is to assist the [HEAD] of the [LEAD AGENCY], or his or her designee, in establishing policies and developing guidelines for the implementation and operation of the SIS to demonstrate the effectiveness of shared management decisionmaking in the collection, storage, and dissemination of criminal intelligence information on a statewide basis.

Furthermore, members of the SIS Control Group shall assist the [HEAD] of the [LEAD AGENCY], or his or her designee, in planning, developing, implementing, and promoting the SIS. The SIS Control Group shall assist the [HEAD] of the [NAME OF LEAD AGENCY] in developing policies, procedures, and practices for the implementation and operation of the SIS. In order to meet these objectives, the SIS Control Group will address the following issues:

- Eligibility of Participating Agencies
- Information Submission Criteria
- Information Inquiry/Access/Dissemination Criteria
- Information Retention/Deletion Criteria
- Security of Information
- Audit Trails

Composition of the SIS Control Group

The [HEAD] of the [NAME OF LEAD AGENCY] will automatically serve as Chair of the SIS Control Group.

The SIS Control Group is comprised of representatives from the following agencies as voting members: [LIST NAMES OF AGENCIES]

The SIS Control Group is also comprised of representatives from the following agencies as nonvoting members: [LIST NAMES OF AGENCIES]

Each voting member agency of the SIS Control Group shall have an equal vote; the SIS Control Group shall strive to achieve unanimous consent for all major decisions. Nonvoting members will provide input but not participate in the voting of the SIS Control Group. The SIS Control Group member will be the [HEAD] of the [NAME OF PARTICIPATING AGENCY]. The [HEAD] of the [NAME OF PARTICIPATING AGENCY] may designate an alternate to represent the [NAME OF PARTICIPATING AGENCY]. The alternate shall have the authority to represent the [HEAD] of the [NAME OF PARTICIPATING AGENCY] in every capacity including voting.

Applicability

As a member of the SIS Control Group, the undersigned agrees to comply with the provisions of the U.S. Department of Justice Criminal Intelligence Systems Operating Policies, 28 CFR Part 23 (September 16, 1993), and will not implement policies or procedures that conflict with the Regional Information Sharing Systems (RISS) Program Guidelines.

Implementation of MOU

Members of the SIS Control Group will serve as a working group, which will meet on a regular basis. The working group may, as appropriate, establish subcommittees comprised of other staff within the participating agencies to address special issues.

Authority

This MOU shall be carried out within the authority of the signing agencies.

Amendments

This MOU may be modified or amended by written agreement between the [HEAD] of the [NAME OF LEAD AGENCY] and the members of the SIS Control Group.

Termination

This MOU may be terminated by mutual agreement of the [HEAD] of the [NAME OF LEAD AGENCY] and the members of the SIS Control Group. If a member of the SIS Control Group chooses to terminate his or her participation in the MOU, he or she can do so by providing a 30-day written notice to the Chair of the SIS Control Group.

As a member of the SIS Control Group, the undersigned agrees to abide by and uphold the conditions set forth in this MOU.

Executed this ____ day of _____, 19__.

[CONTROL GROUP MEMBER NAME]
[TITLE]
[AGENCY NAME]
[AGENCY ADDRESS]

As the designated alternate member of the SIS Control Group, the undersigned agrees to abide by and uphold the conditions set forth in this MOU.

Executed this ____ day of _____, 19__.

[ALTERNATE NAME]
[TITLE]
[NAME OF AGENCY]
Executed this ____ day of _____, 19__.

[NAME OF LEAD AGENCY HEAD]
[TITLE]
[NAME OF LEAD AGENCY]
[ADDRESS OF LEAD AGENCY]
Executed this ____ day of _____, 19__.

Appendix D

Statewide Intelligence System Sample Participation Agreement

This agreement is made and entered into between the [NAME OF LEAD AGENCY], which is responsible for coordinating the Statewide Intelligence System (SIS), and the [NAME OF PARTICIPATING AGENCY] [hereinafter referred to as the Participating Agency].

The [NAME OF LEAD AGENCY] hereby agrees to:

1. Establish and maintain a central computerized statewide criminal intelligence information system for the sole purpose of assisting local, state, and federal law enforcement agency personnel in ongoing multijurisdictional investigations or prosecution activities relating to specific areas of criminal activity. The intelligence system will be known as the [STATE] Statewide Intelligence System (SIS). The [STATE] SIS will develop the necessary computer programs to provide Participating Agencies with system access capabilities.
2. Supply prospective Participating Agencies with membership applications and policy information and, upon attainment of membership, procedural guidelines and necessary forms as adopted by the [NAME OF LEAD AGENCY] and the SIS Control Group, an advisory board to the [NAME OF LEAD AGENCY].
3. Notify the SIS Control Group of any information pertaining to alleged violations of policies and/or procedures by Participating Agencies.
4. Establish criteria, with the advice of the SIS Control Group, for:
 - Eligibility of Participating Agencies
 - Information Submission
 - Information Inquiry/Access/Dissemination
 - Information Retention/Deletion
 - Security of Information
 - Audit Trails

The Participating Agency agrees to:

1. Comply with the U.S. Department of Justice Criminal Intelligence Systems Operating Policies, 28 CFR Part 23 (September 16, 1993), where applicable, and with the policies and procedures promulgated by the [NAME OF LEAD AGENCY] and the SIS Control Group, when utilizing the SIS.
2. Assume responsibility for entering, maintaining, purging, and querying the SIS through approved Participating Agency representative(s) in compliance with the policies and procedures promulgated by the [NAME OF LEAD AGENCY] and the SIS Control Group.
3. Assume responsibility for ensuring that all data submitted for storage in the SIS is connected to known or suspected criminal activity for operation of the system.
4. Assume responsibility for ensuring the accuracy of all information submitted for storage in the SIS.
5. Assume responsibility for ensuring that data determined to be inaccurate, outdated, or otherwise no longer deemed relevant to the objectives of the SIS is immediately purged from the SIS.
6. Assume responsibility for restricting the dissemination of information obtained from the SIS and for any use or misuse of said information.

7. Assume responsibility for all of its actions in the exercise of its rights pursuant to this Participation Agreement and to indemnify and hold harmless the [NAME OF LEAD AGENCY] and its agents from any and all claims, demands, actions, suits, and proceedings by others directly resulting from, or incident to, the Participating Agency's use of the information services authorized by this Participation Agreement.

FURTHERMORE, the parties hereto acknowledge and agree that all submissions of criminal intelligence information on individuals and organizations submitted to the SIS are the property of the submitting agency.

This Participation Agreement will become effective on [DATE] and will remain effective until termination by any of the parties hereto after a minimum of 30 days notice.

IN WITNESS WHEREOF, the parties hereto caused this Participation Agreement to be executed by the proper officers and officials:

[AGENCY NAMES AND SIGNATURES]

Statewide Intelligence Systems Projects

Additional information about the Statewide Intelligence Systems (SIS) projects may be obtained from the SIS projects listed below and from the Institute for Intergovernmental Research.

Tennessee

Tennessee Bureau of Investigation
Criminal Intelligence Unit
1148 Foster Avenue
Nashville, TN 37210
(615) 741-0430

Wisconsin

Wisconsin Department of Justice
Division of Narcotics Enforcement
Post Office Box 7857
Madison, WI 53707-7857
(608) 267-1333

Connecticut

Connecticut State Police
Central Criminal Intelligence Unit
294 Colony Street, Building #9
Meriden, CT 06451
(203) 238-6561

North Dakota

Office of Attorney General
Bureau of Criminal Investigation
Post Office Box 1054
Bismarck, ND 58502
(701) 328-5500

Utah

Utah Department of Public Safety
Division of Investigation
Post Office Box 18654
Salt Lake City, UT 84118
(801) 284-6223

Institute for Intergovernmental Research

Post Office Box 12729
Tallahassee, FL 32317
(850) 385-0600