Exhibit A

INTERIM MEMBERSHIP AGREEMENT
between
Mid-States Organized Crime Information Center

and

Columbia Police Department, Missouri
(Name/State of Agency Entering Agreement)

The Mid-States Organized Crime Information Center® (hereinafter MOCIC) desiring to provide criminal intelligence assistance and information to MOCIC member law enforcement agencies and other participants in the Regional Information Sharing Systems® (hereinafter RISS), does hereby agree to provide that assistance and information to the agency listed above pursuant to the MOCIC Constitution, Article Two.

The above named agency, desiring to receive criminal intelligence assistance and information in the furtherance of its law enforcement activities, and wanting to participate in the exchange of criminal intelligence among member agencies, does hereby agree to all applicable provisions of the MOCIC Constitution and By-Laws and in particular those provisions of Article One, 1(a) and Article Five, "Operations."

As a member of MOCIC and on behalf of the above named agency, I certify that I agree to follow the procedures established in the CONSTITUTION AND BY-LAWS provisions regarding data entry, maintenance, security and dissemination. Further, I agree to verification of these procedures by center staff at the time of membership acceptance, and periodically thereafter, to ensure compliance is maintained.

I further certify that the above named agency also agrees to adhere to the most recent version of those policies and guidelines, which MOCIC and/or RISS shall establish pertaining to specific services, including, but not limited to, the RISS Privacy Policy, MOCIC Member Guidelines for Intelligence Services, MOCIC Equipment Guidelines and MOCIC Confidential Expenditure Operating Guidelines.

I further certify that should the above named agency elect to use the RISS Officer Safety Event Deconfliction System (hereinafter RISSafe) application, that the above named agency will adhere to the most current version of the RISSafe Policy.

Chief Geoffrey Jones
Agency Administrative Head (please print)

MOCIC Executive Director (please print)

Agency Administrative Head Signature

MOCIC Executive Director Signature

Date

Date

Approved as to form: NW

City Counselor

P.O. Box 1250 Springfield, MO 65801-1250
(417) 883-4383 (800) 846-6242
Fax: (417) 883-2154
membership@mocic.riss.net

CONSTITUTION & BYLAWS

2255 W Sunset St
Springfield, Missouri 65801-1250
417-883-4383
800-846-6242

Revision #16 – 10/09

Revisions:

Revision #1 – September, 1982
Revision #2 – September, 1983
Revision #3 – September, 1986
Revision #4 – September, 1987
Revision #5 – September, 1988
Revision #6 – September, 1989
Revision #7 – September, 1990
Revision #8 – September, 1991
Revision #9 – February, 1992
Revision #10 – November, 1992
Revision #11 – July, 1995
Revision #12 – February, 1996
Revision #13 – May, 1997
Revision #14 – January, 1998
Revision #15 – December, 1998
Revision #16 - October, 2009

TABLE OF CONTENTS

CONSTITUTION

BYLAWS

CONSTITUTION

ARTICLE ONE:
NAME

The name of this Organization shall be the **MID-STATES ORGANIZED CRIME INFORMATION CENTER (MOCIC).**

ARTICLE TWO:
PURPOSE AND GOALS

A. The Purpose and Goals of MOCIC shall be:

1. The purpose of MOCIC is to provide information, intelligence and resource support to mid-states federal, state and local law enforcement agencies to combat criminals, organized crime and narcotics trafficking that transverse jurisdictional or state boundaries.

2. The purpose and goals of MOCIC are to reduce the crime committed by criminals, organized crime and illegal drug traffickers whose illegal activities transverse the jurisdictional and state boundaries of Kansas, Missouri, Iowa, Nebraska, North Dakota, South Dakota, Minnesota, Wisconsin and Illinois by establishing a formal information, intelligence and resource repository that will:

   a. Promote cooperation and information exchange among law enforcement member agencies within the mid-states region;

   b. Receive, analyze and disseminate information and intelligence on specific subjects and activities provided by law enforcement member agencies within the mid-states region;

   c. Make available necessary surveillance and communication equipment and monetary resources to enable law enforcement to successfully combat traveling criminals within the mid-states region;

   d. Provide comprehensive training to those law enforcement member agencies participating in the investigation of complex criminal conspiracies and the effective utilization of information, intelligence, equipment and monetary resources provided by MOCIC.

B. In addition to MOCIC's mid-states coordination and analytical roles, MOCIC will maintain an effective means of interface with federal, state and local agencies concerned with the enforcement of criminal law, organized crime and narcotics trafficking across jurisdictional, state and national boundaries.

ARTICLE THREE:
OFFICERS

The Officers of MOCIC shall be:

1. Chairman
2. Vice Chairman
3. Secretary
4. Sergeant-At-Arms
5. Member
6. Member
7. Member
8. Member
9. Member
10. Host Agency Member
11. The MOCIC Director (Ex Officio – Non-voting)

ARTICLE FOUR:
EXECUTIVE COMMITTEE

The affairs of MOCIC shall be managed by an Executive Committee. The Officers named in Article III of this Constitution shall constitute the Executive Committee.

ARTICLE FIVE:
AMENDMENTS TO THE CONSTITUTION

A. **Executive Committee** – The Executive Committee may amend the Constitution by a two-thirds (2/3) vote of the quorum.

B. **Members** – Whenever the Executive Committee amends the Constitution, the members shall have the right to adopt or rescind such amendment or amendments. Such action shall require an affirmative vote of two-thirds (2/3) of the members voting, which shall be conducted by mail.

   1. Any MOCIC member agency may propose an amendment of change to these Constitution and Bylaws immediately by submitting their proposals to the MOCIC Director who will notify all members of the Executive Committee thirty (30) days prior to a regular meeting. Such

proposals shall be referred to the MOCIC Executive Committee Chairman or their designated representative.

2. After a review of each proposed amendment or change for its propriety and feasibility, the Executive Committee Chairman shall direct the MOCIC Director to forward a copy of the proposed change, including findings from these reviews, to each agency's Executive Member for their vote.

ARTICLE SIX: DISTRIBUTION OF PROPERTY ON DISSOLUTION

A. The property of MOCIC is irrevocably dedicated to the purposes herein stated and no part of the net income or assets of MOCIC shall ever be used for benefit of any officer, member, director or staff thereof or to the benefit of any private persons. Upon the dissolution of MOCIC, its assets remaining after payment, or provision for payment of all debts and liabilities of MOCIC, shall be distributed in compliance with grantor guidelines and appropriate law.

B. **MOCIC Files** – MOCIC files shall be maintained in such a manner as to ensure the utmost in security and professional administrative handling. The files shall be regarded as being the property of all contributing member agencies. In keeping with this policy, it shall be understood by all parties concerned that in the event the Mid-States Organized Crime Information Center is abolished, or for other reasons becomes non-operational, all subject specific related materials will be returned to their respective contributing agencies in the most expeditious manner possible. All information and intelligence generated and/or produced by MOCIC will be destroyed. In instances where a change of the host agency occurs, all information and intelligence either contributed by members or produced by project staff will remain the property of MOCIC.

Should membership be voluntarily discontinued or terminated in any manner, it is the agency's responsibility to return all intelligence provided by MOCIC. Further, the agency may, at its discretion, have intelligence submitted to MOCIC returned upon the receipt of a formal request for this action.

BYLAWS

ARTICLE ONE:
MEMBERSHIP AND VOTING

SECTION A Members

1. Application for full membership in the Mid-States Organized Crime Information Center (MOCIC) shall be open to all federal, state and local government law enforcement agencies, organizations and sub-organizations as recognized by federal or state statute as a bonafide law enforcement/police entity within the nine (9) state, mid-states region. Application for limited membership shall be open to federal agencies choosing a limited membership and those Canadian law enforcement agencies whose province is geographically contiguous with that of an MOCIC member state. A limited membership agency is not eligible for the following as related to MOCIC:

    1. Confidential investigative funding
    2. Loan of equipment
    3. Patch call services
    4. To vote or hold office

Limited membership agencies do not pay an annual membership fee.

Acceptance of membership shall be based upon, but not limited to, size of agency, ability of agency to contribute intelligence to MOCIC, ability of agency to participate in cooperative investigations with MOCIC member agencies, ability of agency to gather intelligence, purpose of the agency, proximity of agency to existing member agencies, history of the agency's efforts in conducting intelligence functions, ability of the agency to lawfully exchange general criminal intelligence information and apply high standards of integrity, security and professionalism, and;

a. Certify compliance with the Criminal Intelligence Systems Operating Policies and such other guidelines as necessary to safeguard confidential intelligence information as described in Article Five and other resources provided to them by MOCIC, and;

b. Whose applications for membership in MOCIC are favorably accepted by the State Review Committee, Executive Committee and MOCIC Director.

c. Multi-jurisdictional agencies applying for membership after September 25, 1987 must meet all qualifications stipulated in Article 1, Section A-1.

2. All MOCIC full membership agencies paying annual membership fees shall be active members with the right to vote, hold office and participate in all general membership meetings. There shall be no proxy voting.

3. Each full membership agency paying annual membership fees shall have the right to cast one vote, to be cast by the Executive Member, or in their absence, by the Representative or Alternate member. However, when a MOCIC member agency is a sub-organization of a larger parent organization, that sub-organization will have the right to cast a fraction of one vote in relation to the number of other sub-organizations that are paying MOCIC members. (Note: If the parent organization is also a member, its vote shall be an equal fractional portion of the total number of MOCIC sub-organizations and itself.) The Administrative Head of the parent organization will sign each application from a sub-agency. For example, where the State Crime Bureau and/or State Drug Investigation Unit may be under the auspices of the Attorney General, separate applications can be submitted by these sub-agencies, showing the Attorney General's approval on the application as the Administrative Head.

4. The agency is responsible for returning all intelligence provided by MOCIC and may have intelligence previously submitted to MOCIC returned upon receipt of a formal request for this action.

SECTION B Representative

1. MOCIC member agencies shall have individual members designated by the agency's Administrative Head to serve in the capacities of:

    a. **Executive Member** - As a rule, this will be the highest ranking officer of the law enforcement agency (Commissioner, Chief, Sheriff, Senior Investigator, Supervisor, etc.)

    b. **Representative Member** - As a rule, this will be the officer-in-charge or most senior investigator engaged in intelligence and/or investigation activities directly and/or solely involving criminals, organized crime and/or narcotics trafficking.

    c. **Alternate Member** – As a rule, this will be the second officer-in-charge or second most senior investigator or analyst engaged in

intelligence and/or investigation activities directly and/or solely involving criminals, organized crime and/or narcotics trafficking.

2. The Executive Member may, at their discretion, either appoint themselves or an executive officer as that agency's MOCIC Executive Member, plus one MOCIC Representative and up to two MOCIC Alternates.

3. The Executive Member is charged with the responsibility for implementing the purposes of MOCIC within their agency and ensuring the integrity of all the projects pertaining thereto.

4. The Representative Member is charged with the responsibility of gathering information and intelligence, maintaining the necessary compliance records within their agency, handling correspondence, formulating assistance requests for their agency and responding to requests for assistance from other MOCIC agencies.

5. The Alternate Member is charged with the responsibility of assisting the Representative Member and shall assume the responsibilities of the Representative Member in their absence.

SECTION C Applications and Admission

1. Application for membership in MOCIC shall be made by the Administrative Heads of a prospective agency on MOCIC application forms. Forms may be obtained by telephoning the MOCIC offices. Prospective applicants may use the numbers listed below:

   (417) 883-4383
   (800) 846-6242

2. Application forms may be obtained by written request to MOCIC.

3. When the application is complete, application forms should be returned to MOCIC.

4. The Administrative Head of the applying agency shall, at the time of application, designate their choice of Executive, Representative and Alternate members.

5. The MOCIC Director shall notify members of the Executive Committee and appropriate State Review Committee Members as soon as possible upon receipt of an application for membership.

6. The appropriate State Review Committee shall act upon the application not more than 90 days after receipt of same, and a majority vote of the members of the Review Committee shall be required for approval. After processing by the Committee, the Committee Chairman shall make a recommendation to the Executive Committee for their next regular meeting. The Executive Committee shall act upon the application at the time presented. An affirmative two-thirds (2/3) vote of the Executive Committee shall be required to approve membership. Notification of approval or disapproval shall be made in writing to the applicant agency.

7. If for any reason any designated member from a MOCIC member agency can no longer serve, the Administrative Head of the agency shall notify the Center and provide the name of the replacement.

SECTION D Ethical Conduct

Each MOCIC individual member shall at all times conduct themselves in such a way as to reflect credit upon themselves, the profession of law enforcement and MOCIC.

ARTICLE TWO: EXECUTIVE COMMITTEE

SECTION A Membership and Authority

1. The Executive Committee shall be composed of eleven (11) officers from MOCIC member agencies as follows:

   a. Nine (9) members, one (1) from each of the MOCIC states as elected by majority vote of the MOCIC members from their respective states to serve three year terms. At the First Annual Meeting, one-third (1/3) of the members will be elected for one (1), two (2) and three (3) year terms. Thereafter, elections for three-year terms will be held annually as existing terms expire. The annual election will be conducted in such a manner as to permit each full member agency to cast a vote. Concurrently, one (1) Alternate from each state will be elected by majority vote to serve for the same term as the member. The Alternate will serve in the absence of the member and with the same powers as the member. There will be no proxy voting. The elected Executive Member and Alternate cannot be from the same MOCIC member agency.

b. One (I) member from the Host Agency as appointed by the Chief Executive Officer of the Host Agency and an Alternate to serve in their absence.

c. The MOCIC Director shall be an ex-officio, non-voting member of the Executive Committee.

2. The MOCIC Director shall be appointed by the Executive Committee, subject to successful completion of background and physical examination and a cooperative selection and termination process approved by the MOCIC Executive Committee. The MOCIC Director shall reserve the right to approve the appointment of and termination of all employees under their supervision.

3. In instances where an Executive Committee member cannot serve, the elected Alternate shall serve until the next Annual Election, at which time they may stand for election for a new term or the unexpired term remaining, as appropriate. In instances where both the Executive Committee member and Alternate from a state cannot serve, an Executive Committee member shall be appointed by that state's Review Committee to serve until the next Annual Election, whereupon that state's members will select a Member and Alternate to complete the unexpired portion of the current three (3) year term remaining. In instances where an Executive Committee Alternate from a state cannot serve, an Alternate shall be appointed by that state's Review Committee to serve until the next annual election, at which time, they may stand for election for a new term or the unexpired term remaining as appropriate. In instances where a state's Review Committee appoints an Alternate, that appointment shall be made within four (4) months of the position vacancy. The state's Review Committee may consider any officer in good standing from that state's member agencies for this appointment.

SECTION B Officers

1. The elected Executive Committee will then select members from their body to hold the following offices:

   a. **Executive Committee Chairman** – It shall be the duty of the Chairman to preside at all meetings of the MOCIC Executive Committee. The Chair shall vote only in case of a tie vote. The Chair shall serve one-year terms and no more than three consecutive one-year terms. The Chair shall call meetings of the Executive Committee no fewer than four times per year and special meetings as occasions demand.

   b. **Vice Chairman** – The Vice Chairman shall hold office for one year and shall not serve for more than three (3) consecutive one-year terms. It shall be the duty of the Vice Chairman to preside at all meetings in the absence of the Chairman and to assist the Chairman. In the event of a resignation, suspension or termination of the Chairman, the Vice Chairman shall ascend to the Chairmanship and serve until the next meeting.

   c. **Secretary** – The Secretary shall hold office for a minimum of one year and may be reappointed from year to year. The Secretary shall keep minutes of all meetings, act as parliamentarian, issue notices of meetings and perform all other duties related to their office. The Secretary shall provide copies of the minutes of all MOCIC meetings to Executive Committee members.

   d. **Sergeant-At-Arms** - The Sergeant-At-Arms shall be appointed from the Executive Committee by the MOCIC Executive Committee Chairman at each Annual Meeting for a one-year term and may be reappointed from year to year. The Sergeant-At-Arms shall ensure that only members of good standing are present during the closed sessions of MOCIC meetings and perform other duties as may be assigned by the Executive Committee Chairman.

2. The Executive Committee shall have the authority to select members from their body to fill vacancies in any office at any time.

SECTION C Committees

1. **State Review Committees**

   a. The Executive Committee Member selected by MOCIC members from their state will be the Chairman of that state's Review Committee. The Chairman will appoint at least four (4) members from other MOCIC agencies within the state to serve on that state's MOCIC Review Committee. The Chairman will only vote in the case of tie votes. Members of these State Review Committees shall serve one-year terms, at which time they will be reappointed or replaced by the State Review Committee Chairman.

b. The State Review Committee's duties will include submitting recommendations concerning applications for MOCIC membership from agencies within their state, investigating any detrimental actions of individual members and member departments from their state that negatively affect MOCIC, recommend changes in MOCIC policies and procedures to the Executive Committee and to periodically review MOCIC operating methods and records to refine and improve same for better service to member agencies within their state.

c. Each State Review Committee Chairman shall have the authority to call meetings of that state's Review Committee as occasions require. Meetings shall be held as necessary, but a minimum of one meeting shall be called each year to review participation of MOCIC member agencies within their state.

d. The Chairman of each State Review Committee, in closed session at each Annual Meeting, shall discuss with state members attending, actions of their State Review Committee and other matters of concern since their last Annual Meeting.

2. **Other Committees**

The Executive Committee shall be responsible for the overall implementation of project activities, and may from time to time appoint such other committees as may be necessary.

SECTION D Quorum

A quorum of the Executive Committee exists when six (6) Executive Committee members, excluding the non-voting MOCIC Director, are present.

SECTION E Voting Procedure

To initiate action of the Executive Committee, the following Executive Committee vote shall be required:

1. Admission of members: Affirmative vote of two-thirds (2/3) the quorum.
2. Suspension of members: Affirmative vote of two-thirds (2/3) the quorum.
3. Termination of members: Affirmative vote of two-thirds (2/3) the quorum.
4. Reinstatement of members: Affirmative vote of two-thirds (2/3) the quorum. More than one negative vote is necessary to exclude.
5. Amendments to the Constitution & Bylaws: Affirmation vote of two-thirds (2/3) of the quorum.
6. On all matters not specifically designated: Simple majority of the quorum.

SECTION F Reapplication

Upon change of the Administrative Head, an MOCIC member agency shall reapply for membership. Sponsorship letters are not required for reapplication. The appropriate State Review Committee shall be notified of the reapplication. The Executive Committee shall act on the reinstatement applications in the manner stipulated in Article I, Section C-6.

Membership Agreement

Upon notice of a change of a member agency's Administrative Head, the "acting" Administrative Head shall complete and return an Interim Membership Agreement certifying that they will abide by the MOCIC Constitution and Bylaws and other operating guidelines regarding their agency's participation with MOCIC until such time as a new Administrative Head is named. This agreement, once returned, would become a part of the permanent record of the agency.

SECTION G Suspension – Pending Investigation

A MOCIC member agency may be suspended, pending a regular meeting, by a two-thirds (2/3) vote of the Executive Committee for the following reasons:

a. Acts detrimental to MOCIC or to the law enforcement profession.
b. Improper or indiscreet handling of MOCIC information and/or other resources.
c. Lack of participation in MOCIC activities.
d. Failure to sign and return the reapplication agreement in a timely manner, not to exceed ninety (90) days.

SECTION H Appeal

Any suspended MOCIC member agency shall have the right to appeal and appear before the Executive Committee, State Review Committee and/or such others as may be necessary to conduct a full and complete hearing by giving written notice to the MOCIC Director. Such a hearing shall be held within ninety (90) days after receipt of such notice from the

appealing agency. The MOCIC Director shall notify the Administrative Head and Executive, Representative and Alternates of the appealing agency, all members of the Executive Committee, appropriate State Review Committee and designated others of the date, time and place of the hearing. A two-thirds (2/3) vote of the Executive Committee will be required to overrule the previous suspension of a MOCIC member agency.

SECTION I Reinstatement

An agency that has been terminated from MOCIC membership may request reinstatement. Such a request shall take the form of and be processed the same as a new membership application as stipulated in Article II: Section C. This process may be supplemented with a formal hearing as stipulated in Article I: Section G. The requesting agency will receive formal notification of the results of their application as recommended by the Executive Committee.

SECTION J Voluntary Termination

Agency membership in MOCIC shall be terminated upon receipt of a formal request for such action by the MOCIC Director.

SECTION K Involuntary Termination

Involuntary termination of membership is a last resort. It is assured, therefore, before a problem reaches a magnitude or severity to consider termination, a discussion will be held with the member agency in question. This effort will include the Administrative Head and Executive and Representative members from the agency, Executive and State Review Committee Chairman, the MOCIC Director and such others as might be necessary to accurately determine the full extent of the problem. Such discussions will be preceded by formal notification that involuntary termination is pending and why. A report of the findings will be presented to the Executive Committee by the Chairman. It shall take a two-thirds (2/3) vote of the Executive Committee to terminate any member agency. Should termination occur in this manner, the agency continues to be responsible for returning all intelligence provided by MOCIC and may elect to have intelligence submitted to MOCIC returned by making a formal request for this action.

ARTICLE THREE: AMENDMENTS TO THE BYLAWS

SECTION A Executive Committee

The Executive Committee may amend the Bylaws by two-thirds (2/3) vote of the quorum.

SECTION B Members

Whenever the Executive Committee amends the Bylaws, the members shall have the right to adopt or rescind such amendment or amendments. Such action shall require an affirmative vote of two-thirds (2/3) of the members voting, which shall be conducted by mail.

1. Any MOCIC member agency may propose an amendment of change to these Constitution and Bylaws by submitting their proposals to the MOCIC Executive Director, who will forward the proposal to the Executive Committee thirty (30) days prior to a regular meeting.

2. After a review of each proposed amendment or change for its propriety and feasibility, the Executive Committee Chairman shall direct the MOCIC Director to forward a copy of proposed changes, including their findings and recommendations, to the membership for their vote. Such action shall require an affirmative vote of two-thirds (2/3) of the members voting, which shall be conducted by mail.

ARTICLE FOUR: ANNUAL MEETINGS

SECTION A Annual Meetings

1. The Mid-States Organized Crime Information Center (MOCIC) shall hold an Annual Meeting of MOCIC member agencies. The location of Annual Meetings shall be determined by the Executive Committee and announced to the membership at the close of each Annual Meeting.

2. There shall be at least one closed session each day at each Annual Meeting attended by members only. At least one of these sessions shall be devoted to MOCIC administrative and internal affairs. The proceedings of all closed sessions shall be confidential, and any breach of

this confidence shall result in either termination of the MOCIC member agency's membership and/or individual member responsible.

3. Persons from MOCIC member agencies, prospective member agencies and others as approved by the MOCIC Director may attend all Open Sessions and general training activities conducted at MOCIC Annual Meetings.

SECTION B Executive Committee

The Executive Committee will meet four (4) times yearly to discuss the activities of MOCIC, accept new memberships and resolve matters that require Committee attention.

SECTION C State Review Committee

Each State Review Committee Chairman shall have the authority to call meetings of their state's Review Committee as occasions require. Meetings shall be held as necessary, but a minimum of one meeting shall be called each year to review participation of MOCIC member agencies within their state. The one required committee meeting may be held in conjunction with the Annual Meeting. When held in conjunction with the Annual Meeting, expenses incurred are the responsibility of the appointed Committee Members or their individual agency or department.

ARTICLE FIVE: OPERATIONS

SECTION I

The Office of Justice Programs, Bureau of Justice Assistance, has adopted regulations that apply to intelligence systems funded under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. These regulations are published as Title 28, Part 23 of the Code of Federal Regulations. The Mid-States Organized Crime Information Center (MOCIC) will operate in compliance with these regulations.

SECTION II

The Mid-States Organized Crime Information Center will serve as a central depository for information received from the nine (9) mid-states consisting of Missouri, Kansas, Iowa, Nebraska, South Dakota, North Dakota, Minnesota, Illinois, and Wisconsin and any limited membership agencies. At the initiation of the Mid-States Organized Crime Information Center, law enforcement Administrators representing the nine (9) states involved agreed the information from MOCIC would be disseminated only among authorized law enforcement agencies.

MOCIC member agencies will not use MOCIC equipment for surveillance purposes that is in violation of Title III of Publ. L 90-351, as amended, or any subsequent applicable federal law, or any applicable state statute related to wiretapping and/or surveillance.

A member agency or officer may be suspended from access to MOCIC services, pending a regular meeting by a two-thirds (2/3) vote of the Executive Committee for the following reasons:

1. Acts detrimental to MOCIC or to the law enforcement profession.
2. Improper or indiscreet handling or use of MOCIC information and/or other resources.
3. Lack of participation in MOCIC activities.

Mid-States Organized Crime Information Center (MOCIC) member agencies will be required to certify that they agree to follow the procedures established in the Constitution and Bylaws.

This certification shall be required at the time of an agency's membership, and upon reapplication due to change of the member agency's Administrative Head.

ARTICLE SIX: EXECUTIVE COMMITTEE RULES

The Executive Committee may from time to time make, amend and rescind such rules and regulations as may be necessary to carry out the provisions of its Constitution and Bylaws. A copy of all rules and regulations, and amendments or rescissions thereof, shall be distributed to the MOCIC membership within a reasonable time after their adoption.

REGIONAL INFORMATION SHARING SYSTEMS® (RISS) PROGRAM

Privacy Policy

Contents

August 2013

Approval Date:	Effective Date:	Revision:
August 6, 2009	August 6, 2009	July 5, 2011 (Ratified July 26, 2011) August 21, 2013

Section 1: Introduction and Purpose Statement

The Regional Information Sharing Systems (RISS) Program was established almost four decades ago, primarily to promote law enforcement information sharing. Information sharing is a critical element in effectively and efficiently detecting, deterring, apprehending, and prosecuting criminals and terrorists. Because of the focused effort by law enforcement and criminal justice agencies from all levels of government, numerous improvements have been made in recent years to ensure that the right individuals receive the right information at the right time. The way law enforcement conducts business today is much different, with technology evolving faster each day. It is vital that the law enforcement community have the capability to instantly communicate and share information. Likewise, law enforcement must also protect, respect, and uphold the privacy, civil rights, and civil liberties of individuals.

RISS supports law enforcement and public safety efforts in a variety of ways, including information sharing, investigative research assistance, analytical support, technical equipment loans, confidential funds, training, publications development and dissemination, field services, and technical assistance.

The intent of this RISS Privacy Policy is to protect individual privacy, civil rights, civil liberties, and other protected interests and to address the proper handling of:

- Personally identifiable information (PII) housed in resources maintained and operated by the RISS Program, such as the RISS Criminal Intelligence Databases (RISSIntel™);
- Other criminal justice information available to authorized RISS Center staff, such as criminal history information, suspicious activity reporting (SAR) information, and other investigative information; and
- Personally identifiable information that member agencies, individual officers, analysts, participants, partners, and other entities provide to RISS in order to become a RISS member or participant and to access RISS-related resources and services.

This privacy policy was developed in accordance with the Global Justice Information Sharing Initiative (Global) *State and Local Privacy Policy Development Template: Privacy, Civil Rights, and Civil Liberties Policy Workbook*. In addition, supporting documents, such as the *Fusion Center Privacy Policy Development* document, were reviewed and used, as appropriate. RISS also consulted privacy experts during the development of this policy.

Section 2: Definitions

A. Authorized User—an individual who has successfully completed the RISS identification and approval process or who is accessing RISS resources through an established federated identity partnership and has been granted permissions to appropriate information technology resources available via RISS.
B. Electronic Communication—any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic systems, devices, or services.

C. Fusion Center—a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity. (Source: *Fusion Center Guidelines*)

D. Homeland Security Information—as defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that:
   1. Relates to a threat of terrorist activity;
   2. Relates to the ability to prevent, interdict, or disrupt terrorist activity;
   3. Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
   4. Would improve the response to a terrorist act.

E. Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—a suspicious activity report (SAR) that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). See also Suspicious Activity and Suspicious Activity Report (SAR).

F. Law Enforcement Investigative Purpose—the situation in which data can be directly linked to a criminal justice or law enforcement agency's authorized investigative activity.

G. Need to Know—as a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

H. Participating Agency(ies)—any vetted or approved law enforcement, criminal justice, or public safety entity and private partners utilizing RISS's services, resources, and network. This includes those individuals vetted as ATIX Participants, member agencies, and other partners.

I. Personally Identifiable Information—one or more pieces of information that, when considered together or when considered in the context of how they are presented or how they are gathered, are sufficient to specify a unique individual. The pieces of information include:
   1. Personal characteristics such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometric information such as fingerprints, DNA, and retinal scans.
   2. A unique set of numbers or characters assigned to a specific individual, including name, address, phone number, social security number, e-mail address, driver's license number, financial account, or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System (IAFIS) identifier, or booking or detention system number.
   3. Descriptions of events or points in time, including information in documents such as police reports, arrest reports, and medical records.
   4. Descriptions of locations or places, including geographic information systems (GIS) locations, electronic bracelet monitoring information, etc.

J. Right to Know—based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

K. RISS ATIX™ Participant—executive and official staff from governmental or nongovernmental entities involved with planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism, disasters, or other law enforcement and public safety strategic and tactical response efforts who have successfully completed the RISS identification and approval process for access to RISS ATIX resources.

L. RISS Member Agency—a criminal justice or law enforcement agency or organization approved for membership by a RISS Center policy board and provided access to appropriate RISS services and resources.

M. RISS Secure Cloud (RISSNET™)—RISSNET is a secure sensitive but unclassified (SBU) law enforcement information sharing cloud provider. RISSNET serves as a secure communications backbone and infrastructure for sharing criminal intelligence and other law enforcement and public safety-related information. RISSNET provides a secure platform at the SBU level for communications among agencies, as well as access to various state and federal criminal intelligence and information systems across the country.

N. RISSNET Node/Node Partner—any local area network (LAN) or wide area network (WAN) electronically connected to RISSNET infrastructure via (1) a dedicated communications circuit and a RISSNET-compliant firewall or (2) an Internet Protocol Security/Virtual Private Network (IPsec VPN) connection and a RISSNET-compliant router.

O. Suspicious Activity—observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. (Source: ISE-SAR Functional Standard (Version 1.5)) Examples of suspicious activity with a potential nexus to terrorism include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

P. Suspicious Activity Report (SAR)—official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for supplying information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Q. Terrorism Information—consistent with Section 1016(a)(5) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals. Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

R. Terrorism-Related Information—in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the Office of the Program Manager, Information Sharing Environment (PM-ISE), facilitates the sharing of terrorism and homeland security information, as defined, respectively, in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as

defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include criminal intelligence information.

Section 3: Governance and Oversight

RISS is a congressionally funded program administered by the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA).

The RISS National Policy Group (RNPG) is composed of the six RISS Center Directors and the chair of each RISS Center's policy board. The RISS Center's policy board (or executive committee) is established by each RISS Center and composed of representatives from member criminal justice agencies in the center's geographic service area. The primary purpose of the board is to provide direction affecting center policy, operation, and administration.

The primary purpose of the RNPG is to provide direction affecting RISS Center policies, operations, and administration. The RNPG is responsible for strategic planning, resolution of operational issues, advancement of information sharing, and other matters affecting the RISS Program and RISS Centers. Each of the RISS Directors, individually and collectively, is responsible for the overall operation of the RISS Program, including its justice information systems, information collection and retention procedures, coordination of personnel, and enforcement of this policy.

Section 4: RISS Owned and Operated Information Technology Resources

RISS has developed and continues to maintain and operate a number of intelligence and investigative resources to assist and support law enforcement and public safety entities. The following resources include electronic systems or databases available to authorized users via RISSNET:

- RISS Criminal Intelligence Databases (**RISSIntel**), as well as various state, regional, federal, and specialized criminal justice information systems. (Note: While RISS operates RISSIntel, RISS does not maintain or operate these individual state, regional, federal, and specialized criminal justice information systems.)
- The 7th Instance of the RISS Suite of Applications (RISSApps), known as **RISS7**—an alternate criminal intelligence database for deployment and use in law enforcement agencies to store collected criminal intelligence data.
- RISS National Gang Program (**RISSGang**™)—consists of a gang-related criminal intelligence database, secure communications tools, and a secure website.
- RISS Automated Trusted Information Exchange™ (**RISS ATIX**)—includes secure web pages, a discussion forum, a document library, and secure e-mail for law enforcement and public safety entities.
- RISS Officer Safety Event Deconfliction System (**RISSafe**™)—stores and maintains data on planned law enforcement events with the goal of identifying and alerting affected law enforcement agencies to potential conflicts with other law enforcement agencies' events.

- RISS Officer Safety Website—serves as a national repository for officer safety information and resources, including concealments, hidden weapons, armed and dangerous threats, officer safety videos, special reports, and training opportunities.
- RISSLeads Investigative Website™—provides a secure electronic bulletin board that enables users to post information on a case or raise or respond to other law enforcement issues.
- Data Visualization and Link Analysis Tool (**RISSLinks**™)—provides an analytical chart when a record is viewed by a user in RISSIntel that visually depicts the associations between people, places, and things.
- Other resources include the RISS search engine (**RISSearch**), individual RISS Center websites, and secure e-mail.
- Other information technology resources operated by individual RISS Centers, such as investigative databases.

A. 28 Code of Federal Regulations (CFR) Part 23 Compliance

1. RISS firmly recognizes the need to ensure that individuals' privacy, other civil liberties, and civil rights are protected throughout the intelligence and information sharing process.
2. RISS endorses the *National Criminal Intelligence Sharing Plan's* (NCISP) guideline that ensures that "the collection, submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations" and that "law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies federal regulation (28 CFR Part 23)."
3. RISS Centers have adopted policy guidelines that fully comply with 28 CFR Part 23. All RISS member agencies have also agreed, in writing, to comply with the requirements of 28 CFR Part 23 with respect to any criminal intelligence information they submit into or receive from applicable RISS criminal intelligence databases.
4. RISS criminal intelligence databases are maintained in compliance with 28 CFR Part 23. This includes requirements governing receipt, storage, and maintenance of criminal intelligence information; exclusion of illegally obtained information; restrictions on dissemination; observance of administrative, technical, and physical safeguards (including establishment of audit trails); review and purge requirements; and forbidding the purchase or use of any electronic, mechanical, or other device for surveillance that is in violation of the provisions of the Electronic Communications Privacy Act of 1986 or applicable state law related to wiretapping or surveillance.

B. Policy Applicability and Legal Compliance

1. **RISS Staff**—RISS staff will be provided a printed or electronic copy of this policy. Staff will acknowledge receipt of this policy by e-mail notification or other appropriate method. By acknowledging receipt of this policy, staff members agree to comply with this policy and with applicable laws and regulations protecting privacy, civil rights, and civil liberties.
2. **Partners/Contractors/Others**—RISS participating agencies, users, partners, contractors, and others, as appropriate, will be governed by participation applications, user agreements, and contracts, which will comply with the provisions of this policy and with applicable laws protecting privacy, civil rights, and civil liberties. Relevant portions of this policy will be

included in agreements and contracts. Agreements and contracts will reference the full policy and its location.

3. A copy of the RISS Privacy Policy will be made available upon request. The latest version of this policy will be posted at the RISS public website, www.riss.net.

C. New Information Technology Initiatives

1. The RNPG or individual RISS Centers may partner with other criminal justice entities to enhance information sharing programs or develop new programs and initiatives that further the RISS Program's mission and goals. The RNPG, a RISS Center Director, or the RISS Technology Support Center (RTSC) Manager will conduct, as appropriate, a privacy assessment of new or emerging initiatives. RISS will leverage the Global *Guide to Conducting Privacy Impact Assessments (PIA) for State, Local, and Tribal Information Sharing Initiatives* for this purpose.
2. The PIA will be completed, as appropriate, by the RNPG, the appropriate RISS Center, or a designee and will be maintained by the RNPG, the RISS Center, or a designee.
3. Annually, RISS will adjust, as required, the project strategy, technology specifications, this privacy policy, and/or other appropriate operating policies and procedures to ensure that privacy, civil rights, and civil liberties are protected in the implementation of a new or expanded information sharing program or initiative.

D. RISS Database Information Collection

1. Data submitted to RISSIntel, the RISSGang intelligence database, RISSafe, RISS7 instances, or any other RISS-maintained database is owned by originating agencies.
2. RISS and participating agencies using the RISS databases shall comply with and adhere to all laws and regulations, including, but not limited to:
   a. 28 CFR Part 23 regarding collection of criminal intelligence information.
   b. The Organisation for Economic Co-operation and Development's Fair Information Principles (FIPs) (http://it.ojp.gov/documents/OECD_FIPs.pdf), which include:

      - Collection Limitation Principle
      - Data Quality Principle
      - Purpose Specification Principle
      - Use Limitation Principle
      - Security Safeguards Principle
      - Openness Principle
      - Individual Participation Principle
      - Accountability Principle

   c. NCISP recommendations regarding information and intelligence sharing.
   d. Applicable constitutional, statutory, regulatory, and administrative rules and other legal provisions, as well as any other DOJ regulations that apply to multijurisdictional criminal intelligence databases.
3. External agencies that access and share information with the RISS Program shall comply with the laws and regulations governing those individual agencies in addition to this privacy policy, other RISS policies, and applicable laws and regulations.
4. RISS will partner only with entities that provide appropriate assurances that their methods for gathering personally identifiable information comply with applicable laws and regulations and that these methods are based on lawful information collection practices.

5. RISS will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.
6. To the maximum extent possible, information received from RISS by originating agencies will be labeled (by record, data set, or system of records), pursuant to applicable limitations on access and sensitivity of disclosure to:
   a. Protect confidential sources and police undercover techniques and methods.
   b. Not interfere with or compromise pending criminal investigations.
   c. Protect an individual's right of privacy and his or her civil rights and civil liberties.
   d. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

E. Data Quality

1. RISS will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate, current, and complete, including the relevant context in which it was sought or received and other related information; and properly merged with other information about the same individual or organization. (See Section 4. G. below pertaining to merging/linking of records information.)
2. Originating agencies external to RISS are responsible for the quality and accuracy of the data accessed by or provided to RISS. If data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable, RISS will advise the appropriate contact person, in writing or electronically, in the originating agency. The originating agency is responsible for then confirming (as accurate), correcting, or purging the information from the RISS resource within a reasonable time. Recipients of the information will be notified of errors or deficiencies that may affect the rights of the subject of the information.
3. Depending upon the resource (e.g., RISSIntel, RISSGang, RISSafe), data provided by authorized users to RISS-supported systems shall:
   a. Be based on proper criminal predicate or threat to public safety;
   b. Be based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal or terrorist activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity;
   c. Be relevant to the investigation and prosecution of suspected criminal or terrorist incidents; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
   d. Be relevant in a criminal analysis or in the administration of criminal justice and public safety (including topical searches);
   e. Support authorized public safety and private sector efforts, as appropriate, and facilitate information sharing and communications among these entities; or
   f. Protect officer safety and ensure the integrity of investigative efforts.

   The data shall also be derived from a source that is reliable and information that has been verified or where limitations on the information's quality are identified. The information

must be collected in a lawful manner, with the knowledge and consent of the individual, if appropriate.

F. Collation and Analysis

1. Users submitting information to RISS-supported systems are authorized individuals from member agencies or appropriate nonmember law enforcement, public safety, or private sector entities. These individuals are sworn law enforcement officers, intelligence analysts, criminal justice officials, public safety officials, and appropriate critical infrastructure and private entity officials.
2. As necessary, RISS may provide limited information, such as contact phone numbers, to appropriate RISS members to facilitate communications and enhance information sharing. For example, ATIX Participant information is provided at the secure ATIX website for participants to obtain phone numbers of individuals addressing similar public safety issues. (See Section 6 for additional information.)
3. Users are permitted to access only information and systems specifically authorized for their use.
4. Information acquired or received by RISS or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly.
5. RISS may acquire or receive the following types of information: criminal intelligence, criminal history, investigative case information, SBU information, other investigative data (such as information housed in the RISS Pawnshop Database, the Pseudo Violator Tracking System, and the Cold Hit Outcome Project), terrorism-related suspicious activity reports, and public record information.
6. Information acquired or received by RISS or accessed from other sources is analyzed according to priorities and needs to:
   a. Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and other priorities established by RISS;
   b. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal or terrorist activities;
   c. Support investigations, including those of gang activity, criminal violence, illegal narcotics, cybercrime, terrorism, human trafficking, identity theft, and other appropriate crimes;
   d. Support and facilitate public safety and private sector efforts safeguarding critical infrastructure and responding to disasters; or
   e. Ensure officer safety.

G. Merging/Linking of Records

1. Records regarding an individual or organization from two or more sources will not be merged by RISS Center staff.
2. Records may be linked by authorized RISS personnel when there is sufficient identifying information to reasonably conclude that the information is about the same individual or

organization. In order to link information, authorized RISS personnel shall review all available attributes and ascertain a set of identifiers that support a high degree of accuracy.

H. Access

1. Credentialed, role-based access criteria will be used by RISS, as appropriate, to control:
   a. The information to which a particular group or class of users can have access based on the group or class.
   b. The information a class of users can add, change, delete, or print.
   c. To whom, individually, the information can be disclosed and under what circumstances.
2. RISS employs and continuously reviews and refines appropriate security and privacy control measures—including physical, electronic, and organizational measures—to ensure that individual identification information is safeguarded and is not compromised.
3. All individuals having access to RISS resources agree to the following:
   a. Criminal intelligence and law enforcement databases accessible via RISSNET will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.
   b. Individual passwords will not be disclosed to any other person.
   c. Individual passwords will be changed if authorized personnel of the agency suspect the password has been improperly disclosed or otherwise compromised.
   d. Use of RISS in an unauthorized or illegal manner will subject the user to denial of further use of RISS resources, discipline by the user's employing agency, and/or criminal prosecution. Each authorized user understands that access to RISS can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.
4. Users are permitted to access only information and systems specifically authorized for their use.
5. Users must complete an Individual User Agreement or equivalent application or acknowledgement or be covered by an interagency Memorandum of Understanding (MOU), in conjunction with training provided.
6. RISS retains the right to suspend or withdraw membership and user privileges, as deemed appropriate, in instances of violation of this or any other RISS policy.
7. All users are subject to the RISS Privacy Policy, the RISSNET Security Policy, the RISSNET Electronic Communications Policy, the RISSNET Remote User Authentication and Access Control Policy, and other RISS-related policies.
8. Use of RISSNET is limited to those individuals who have successfully completed the RISS identification and approval process or who are part of an interagency MOU and have received appropriate training (users).
9. In order to confirm the identity of individual RISSNET users and to ensure that user impersonation is prevented, RISSNET users must provide a variety of personal information about themselves to enable RISS to ensure that only appropriate individuals are permitted access to information for which they have a "need to know" and "right to know." Personally identifiable information provided by authorized users for this purpose, including membership and user information, shall be protected under this policy. (See Section 6 for additional information.)

I. Security

1. RISS will operate secure facilities, whereby personnel maintain appropriate identification to enter the facility and visitors are required to check in and sign in upon entry. The facilities must also meet all appropriate local and state laws and ordinances.
2. RISS will ensure that security procedures are in place in order to safeguard human life and property.
3. RISS will employ secure internal and external safeguards against network intrusion.
4. Access to RISSNET resources will be allowed using only secure networking technologies, such as RISSNET's IPsec VPN or RISSNET's Multiprotocol Label Switching (MPLS) circuits.
5. RISS will grant access to its resources only to RISS staff or appropriate personnel whose positions and job duties require such access.
6. RISS will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
7. Queries made to RISS's data applications will be logged into the data system identifying the user initiating the query.
8. RISS will utilize watch logs to maintain audit trails of requested and disseminated information.
9. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
10. If information is believed to have been breached or obtained by an unauthorized person and access to such information threatens physical, reputational, or financial harm to another person, RISS will notify the originating agency of the breach. The originating agency will notify the individual about whom personal information was breached or obtained. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release. The originating agency will notify RISS that notification was made.

J. Use

1. Use of RISS resources is limited to those individuals who have successfully completed the RISS identification and approval process or who are part of an interagency MOU and have received appropriate training (users).
2. Information obtained through RISS can be used only for the lawful performance of duties and/or for the purposes necessary for effective administration of RISSNET and RISSNET resource authentication and access control procedures.
3. Information obtained through or stored by RISS cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

K. Training

1. **RISS Staff**—RISS will ensure that appropriate staff is trained on this privacy policy.
   a. Training will address the substance of the policy and its importance to RISS's mission and staff members' responsibility, including potential consequences of violating the policy.
   b. The level and amount of training for RISS staff will be based on a staff member's position and access/use of investigative and intelligence data. At a minimum, RISS staff members will complete the 28 CFR Part 23 Online Training course, review and acknowledge the RISS Privacy Policy, and agree to comply with the tenets of this policy.
   c. Additional training will be provided for staff members with direct contact with investigative or intelligence data.
2. **Partners/Contractors/Others**—RISS and the partnering entity will discuss appropriate provisions of this policy during the initial planning and negotiations phase. Member agencies, users, contractors, and other partners are expected to review the tenets of their agreements with RISS, which will include appropriate language from this policy and refer to the full policy and its location.
3. A copy of the RISS Privacy Policy will be made available upon request. The latest version of this policy will be posted at the RISS public website, www.riss.net.

Section 5: Other Investigative Databases and Sources

Each RISS Center employs personnel with expertise in intelligence research, analytical services, law enforcement, criminal justice, and information technology. In order to meet the mission of the RISS Program, RISS Center staff, on behalf of member law enforcement officers, access, utilize, search, analyze, and compile information from a variety of data sources, including those developed and operated by RISS—as well as other data sources—such as commercial databases, motor vehicle records, investigative databases, deconfliction, criminal history information, and suspicious activity reporting (SAR) information.

Investigative data sources that are not owned and operated by RISS may be used by authorized RISS Center staff to assist member law enforcement officers in identifying investigative leads; locating suspects, witnesses, victims, addresses, phone numbers, and other critical elements of a target; developing analytical products; and to assist in furthering an investigation. RISS does not gather, collect, or seek information to populate these resources. Access to these resources is based on a "need-to-know" and "right-to-know" basis. Authorized RISS Center staff are permitted to only query these sources and view records; they may not edit data in these sources. However, RISS staff may conduct analyses and develop intelligence briefings or materials, as requested by an officer. If terrorism-related SAR data is included in that package, the information must comply with the collection, retention, and purge policies pertaining to such data and contained in this policy.

A. Investigative and Commercial Databases

1. Each RISS Center has obtained access to a variety of investigative and commercial databases used to obtain subscription and other investigative information.

2. RISS will partner only with entities that provide appropriate assurances that their methods for gathering personally identifiable information comply with applicable local, state, territorial, federal, and tribal laws and regulations and that these methods are based on lawful information collection practices.
3. RISS will make every reasonable effort to ensure that information obtained from these resources is derived from dependable and trustworthy sources; accurate, current, and complete, including the relevant context in which it was sought or received and other related information; and properly merged with other information about the same individual or organization. (See Section 4. G. pertaining to merging/linking of records for more information.)
4. Originating agencies external to RISS are responsible for the quality and accuracy of the data accessed by or provided to RISS. If data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable, RISS will advise the appropriate contact person, in writing or electronically, in the originating agency.

B. Suspicious Activity Information

1. As part of the Nationwide Suspicious Activity Reporting Initiative (NSI), RISS Center staff may be granted access to terrorism-related suspicious activity reporting information (also known as an Information Sharing Environment Suspicious Activity Report—ISE-SAR) contained in the NSI ISE-SAR shared space.
2. Authorized RISS Center staff shall be granted VIEW-only rights and will not be authorized to download, populate, or edit data.
3. Only RISS Center staff who have successfully completed NSI-approved analyst/investigator training shall be provided access to the NSI ISE-SAR shared space.
4. At the request of a member agency officer, RISS Center staff may query the NSI ISE-SAR shared space. Results will be provided back to the requesting officer, along with any other appropriate results from other sources.
5. RISS will store and provide access to ISE-SAR information using the same method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
6. RISS will utilize this information for law enforcement purposes only and comply with all aspects of this policy in the use and dissemination of such data.

Section 6: Agency and User Information

Officers, analysts, and other appropriate users provide personal identifiers in order to receive access to RISSNET-related resources. Information includes, but is not limited to, the following:

1. Name
2. Title/Rank/Position
3. Organization/Agency/Department, Address, Phone Number, and Fax Number
4. Date of Birth/Place of Birth
5. Cell Phone
6. E-Mail Address(es)

7. Personal Challenge Questions (facts about a user that are not common knowledge and not likely to change)

This information is gathered in order to provide access to RISS's automated resources, as well as other services and programs. RISS maintains this information in a secure environment and utilizes this information only in its mission to provide support and services to law enforcement and other criminal justice entities, to further information sharing, to ensure compliance with this policy and other appropriate laws and regulations, and for auditing purposes.

RISS shall not sell, publish, exchange, or disclose user information without prior approval of the officer, analyst, or appropriate individual.

RISS Center staff will regularly review membership and participant information to ensure accuracy. RISS will make every effort to ensure that the information is accurate and complete. RISS will request updates from agencies and update/delete records as agency contacts change, officers/analysts leave employment, etc.

Agency and user information is also subject to Section 4 of this policy.

Section 7: Audits

A. Section 4 of this privacy policy addresses RISS criminal intelligence databases regarding compliance with 28 CFR Part 23. RISS shall abide by the auditing requirements within that guideline.
B. Systems that are not required to be 28 CFR Part 23-compliant, such as investigative databases, will maintain an appropriate electronic log or auditing capability where available.
C. RISS will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
D. Queries made to RISS's data applications will be logged into the data system identifying the user initiating the query.
E. RISS will utilize watch logs to maintain audit trails of requested and disseminated information. RISS will routinely monitor logs for indications of unusual activity and take appropriate action, if necessary.
F. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

Section 8: Evaluation and Monitoring

A. RISS will continuously evaluate and monitor its resources, technologies, security practices, and associated processes to ensure compliance with this and all appropriate RISS policies.
B. RISS will, through its six RISS Centers, conduct 28 CFR Part 23 compliance reviews of member agency processes. DOJ or RISS may request a third party to conduct additional reviews, as needed and appropriate.
C. RISS will ensure that only appropriate personnel have access to staff, member, and user information.

D. RISS will revise its practices, as appropriate, to ensure continued compliance and to stay abreast of issues impacting the privacy policy arena in order to ensure that all RISS policies and practices are up to date and appropriate.
E. RISS will adopt and follow procedures and practices to ensure and evaluate the compliance of users in abiding by the provisions in this policy and with applicable law. This will include regular audits of the information and intelligence.
F. Requests or questions regarding this policy may be directed to the individual RISS Director covering the appropriate region. A list of the RISS Directors and their contact information is provided at www.riss.net.

Section 9: Accountability

A. RISS Center staff or authorized users shall report violations or suspected violations of this policy to their immediate supervisor, as well as to the in-region RISS Center. The in-region RISS Center Director may resolve the matter as appropriate, engage assistance and consultation from the other Directors, and/or seek legal support to resolve the issue. Items arising that may impact all of the centers or the RISS Program's national initiatives shall be discussed and deliberated by the RNPG for resolution.
B. If an authorized user is found to be in violation of the provisions of this policy, the RISS Center reserves the right to suspend or discontinue access to information by the user and/or request that the relevant member or nonmember agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
C. If any RISS Center staff member is found to be in violation of any provision of this policy, the RISS Center will reprimand, suspend, demote, transfer, or terminate the individual, as authorized by applicable personnel policies.
D. In case of user or staff violations of the law, the RISS Center will refer the matter to appropriate authorities for criminal prosecution, as necessary, to comply with the law and effectuate the purposes of this policy.

Section 10: Revision and Amendments

A. The RNPG has the authority to amend any part(s) of this policy, as appropriate.
B. At least annually, the RNPG will review this policy for content, relevancy, and effectiveness and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy, making appropriate changes in response to implementation experience, changes in applicable law and technology, the purpose and use of the information systems, and public expectations.
C. A representative from a RISS Center, a RISS Director, the RISS Chief Information Officer (CIO), the RTSC Manager, or other appropriate entity may request a change or revision to this policy by contacting the chair of the RNPG and will provide details regarding the proposed change and the reason/justification for the change. The requestor will provide feedback/discussion on the issue. Once any change is approved by the RNPG, the change will be made to this policy and a new version of this policy will be distributed. The staff, users, members, and other participants and partners will adhere to the most recent version of this privacy policy.
D. If changes occur to related policies, laws, or regulations, such as other RISS policies or 28 CFR Part 23, the RNPG may revise this policy, as appropriate.
E. Approved amendments to this policy shall be documented in appropriate RISS meeting minutes, and the date of such action shall be logged herein.

Mid-States Organized Crime Information Center ®

MOCIC MEMBER GUIDELINES

For

INTELLIGENCE SERVICES

May 2017

TABLE OF CONTENTS

The following guidelines will assist members of the Mid-States Organized Crime Information Center (MOCIC) in using MOCIC intelligence resources. These guidelines include both policies and procedures that will ensure prompt, thorough and legally compliant intelligence support to our members. If you have questions about these guidelines or suggestions for improving our service, please contact the Intelligence Supervisor at (800) 846-6242, ext. 4140.

MOCIC provides a number of useful intelligence-sharing tools to its member agencies. As part of the Regional Information Sharing Systems® (RISS), MOCIC's intelligence database (RISSIntel) is one component of the secure, nationwide RISS information-sharing system (RISSNET™). MOCIC/RISS databases are designed to comply with applicable federal laws and policies and MOCIC member agencies have access to the database, as well as all the other elements of the RISSNET system.

On November 2004, all RISS National Gang Database (RISSGang) intelligence was integrated into the RISSIntel database in an effort to streamline criminal intelligence searches. In November 2005, the RISSIntel database structure changed allowing all RISSGang records to remain consolidated within the RISSIntel database, yet be stored as a separately accessible subset of the RISSIntel database. Given the increasing problems with gangs nationwide, and in an effort to share national gang information with as many law enforcement and criminal justice agencies as possible, RISS has decided to provide access to the separately stored RISSGang portion of the database to identified and vetted law enforcement and criminal justice professionals, whether or not they are RISS members. RISSIntel now houses all types of intelligence, including gang intelligence.

In a February 24, 2004, press release, the Department of Homeland Security referenced the RISS system as "law enforcement's premier criminal database." An impressive feature of the RISSIntel database is RISSLinks™, which permits member officers to view the complex, written intelligence contained in member submissions in a link chart that visually depicts the associations between people, places and things.

MOCIC performs three primary intelligence functions: Maintenance of a regional intelligence database, assistance in locating additional intelligence and analysis of intelligence.

Maintenance of the intelligence database is a critical function that is wholly dependent on members' high quality **intelligence submissions.** *All* of the information contained in the RISS database originates from members' intelligence submissions. Therefore, the quality of the information contained in the database is dependent on the quality of the information submitted. Members may telephone **information assistance requests** to MOCIC or remotely access the RISS database for information from members' intelligence submissions. **Intelligence analysis** involves organizing and interpreting criminal intelligence or investigative case material to extract meaning from the information. Analysis is the process of simplifying highly complex information to find the critical elements.

Another effective tool for sharing intelligence is the RISSLEADS Investigative Website. RISSLeads is designed to provide law enforcement a means of secure communication that crosses jurisdictional boundaries quickly and efficiently. Officers can share intelligence with

and seek case assistance from officers across the United States who are connected remotely through the RISS Secure Cloud (RISSNET). RISSLeads is on RISSNET, so only authorized law enforcement users can access the posted information. The retention period for information posted to any of the conference categories is limited and postings to RISSLeads are not required to meet 28 CFR Part 23 requirements. Contact an MOCIC Criminal Information Specialist if you do not have remote connection, but want to use RISSLeads.

All of these functions and other types of support are available to MOCIC member agencies by simply calling MOCIC at (800) 846-6242. The following pages present information necessary to use these services.

I. LEGAL REQUIREMENTS

A. 28 CFR Part 23 – Basic Requirements

Many activities of MOCIC/RISS are governed by the Code of Federal Regulations (CFR), specifically 28 CFR Part 23, Criminal Intelligence Systems Operating Policies (included in this guideline as **Appendix E**). The basic requirements of this regulation are summarized below, with additional explanation regarding its application provided later in this guideline. 28 CFR Part 23 requires that:

- There must be "reasonable suspicion" that a criminal activity occurred or is occurring that is multijurisdictional. **MOCIC policy requires the criminal activity be either felony-level or meet the criteria for "serious misdemeanor criminal activity" as defined by this guideline.**

- Associates submitted must be suspected of criminal involvement with the primary suspect or be suspected of other criminal activity.

- Businesses or organizations submitted must be considered involved in criminal activity or exist for the purpose of criminal activity.

- In certain situations, non-criminal identifying information is allowed, but must be marked as such.

B. Targeted Criminal Categories

28 CFR Part 23 addresses several targeted criminal categories for inclusion in criminal intelligence operating systems. These categories as implemented by MOCIC are summarized below:

1. Individual Suspects

Individuals whose participation in or association with criminal activity traverses jurisdictional boundaries.

For our purposes, jurisdiction is defined as any area (municipality, county or state) with an established law enforcement authority that is in the nine-state area served by MOCIC (Missouri, Kansas, Nebraska, South Dakota, North Dakota, Minnesota, Wisconsin, Iowa, Illinois, and Manitoba, Canada) or the areas served by the other RISS centers (WSIN, RMIN, MAGLOCLEN, ROCIC and NESPIN). See page 23 for more information about the other five RISS centers and their service regions.

2. Organized Criminal Groups

Individual groups, gangs or organizations whose participation in or association with criminal activity involves actual or attempted collusion, association or involvement in a criminal enterprise.

For our purposes, organized criminal groups are defined as any organized group that functions to support, direct or allow criminal activity by its members. You may elect to designate gang intelligence for inclusion in the RISSGang database (see page 11).

3. Illegal / Dangerous Drugs

Individuals, groups, organizations or gangs engaged in producing, possessing, transporting, distributing or selling any illegal drug or controlled substance.

4. Multijurisdictional Criminals

Individuals, groups, gangs or organizations suspected of committing criminal activity, where all or a substantial portion of the criminal activity and/or the impact of the criminal activity occurs in more than one jurisdiction.

5. **Criminal Associates**

Individuals who are suspected of committing criminal activity with others or meet the reasonable suspicion test of 28 CFR Part 23 criteria on their own merit and associate with individuals involved in criminal activity.

C. Criteria for Inclusion

The minimum information required for an authorized contributor to input data into the RISS intelligence database is a **criminal activity** (event) and a **criminal entity** (suspect, group/organization, vehicle, phone number, location, or weapon) associated with that event. The contributor must also indicate the source and content reliability of the information and the information must meet the following tests:

The criminal entity must be **reasonably suspected** of involvement in one or more felony or "serious misdemeanor" criminal activity(ies). The statutes in the submitting agency's jurisdiction determine whether a particular offense is a felony or a misdemeanor. The phrase "serious misdemeanor criminal activity" means those types of criminal activity that could impact more than one jurisdiction and are connected with or have the potential to lead to more aggravated and/or felony-level criminal activity.

MOCIC strives to ensure that its intelligence database contains intelligence submissions that are timely, reliable, relevant and of high utility to law enforcement. During the quality control process, MOCIC may determine that a submitted misdemeanor criminal activity does not meet the "serious misdemeanor criminal activity" criteria and may exclude such submission from the intelligence database.

The following examples are designed to guide you in determining whether a misdemeanor criminal activity meets the criteria for "serious misdemeanor criminal activity." Examples include:

- Prostitution, when connected with one or more additional types of organized felony-level criminal activity.
- Stalking, when the activity is part of a pattern of behavior that has the potential to escalate into more aggravated felony-level activity or that poses a threat to public and/or officer safety.
- Indecent exposure, when the activity is part of a pattern of behavior that has the potential to escalate into more aggravated felony-level activity or that poses a threat to public and/or officer safety.
- Window peeping or other invasion of privacy crimes, when the activity is part of a pattern of behavior that has the potential to

escalate into more aggravated felony-level activity or that poses a threat to public and/or officer safety.

- Theft, when the activity consists of one or more instances that occur within a short span of time and the total loss, in the aggregate, constitutes felony-level criminal activity.
- Possession of narcotics or narcotics paraphernalia that indicates more than illegal recreational use.
- Assault, when connected with one or more additional types of organized felony-level criminal activity or if part of a pattern of behavior that has the potential to escalate into more aggravated felony-level activity or that poses a threat to public and/or officer safety.
- Certain weapons possessions, when connected with one or more additional types of organized felony-level activity or if part of a pattern of behavior that has the potential to escalate into more aggravated felony-level activity or that poses a threat to public and/or officer safety.
- Harassment, when the activity is part of a pattern of behavior that has the potential to escalate into more aggravated felony-level activity or that poses a threat to public and/or officer safety.
- Most traffic-related crimes do not meet the criteria and will not be accepted for inclusion in the intelligence database.

If you have questions about whether a misdemeanor criminal activity is eligible for submission, please call the Intelligence Supervisor at (800) 846-6242, ext. 4140.

Reasonable suspicion is "established when information exists that presents sufficient facts to give a trained law enforcement or criminal investigating 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." This is the threshold test for all information contained in the RISS intelligence database. It is typically less than probable cause and is determined by the contributing officer.

At least a portion of the criminal activity described above or a substantial portion of the impact of the criminal activity must occur within the boundaries of the regions served by MOCIC (see page 6) or the other RISS centers (WSIN, RMIN, MAGLOCLEN, ROCIC and NESPIN). See page 23 for more information about the other five RISS centers and their service regions.

D. Restrictions on Inclusion

The following restrictions apply to all information collected, retained and disseminated by any RISS center:

1. Only information that is relevant to the criminal activity of the individual, group, business, organization, gang or other entity will be included in the RISS intelligence database. Relevant information is that which describes the entity and event in sufficient detail to allow the information to be entered, stored and retrieved for future use. Information on non-criminally associated entities, such as a non-criminally associated employer's name and address or a non-criminal associate's name and address, may be maintained for identification purposes ***only*** if such information is clearly identified as non-criminal identifying information and is essential to the description of the criminal activity.

2. No information or intelligence will be accepted or maintained regarding a suspect's political, religious or social views, race, sexual preference, associations, corporations, businesses, or partnerships, unless such information directly relates to the criminal activity and the need for its inclusion can be clearly explained.

3. All information submitted for inclusion in RISS intelligence database must be obtained in compliance with all applicable federal, state and local laws or ordinances, including, but not limited to, the Electronic Communications Privacy Act of 1986.

4. Federal regulation 28 CFR Part 23 has no limitation or restriction on entering intelligence on juvenile suspects. However, state law may restrict or prohibit the maintenance or dissemination of such information by its law enforcement agencies.

   For purposes of these guidelines, the term "juvenile" is determined by the laws and regulations of the submitting agency's state. As of the current date of these guidelines, this term means any individual younger than 18 years of age, or in the case of Illinois, Missouri and Wisconsin, under 17 years of age.

   MOCIC will allow MOCIC members to submit information involving juvenile subjects to RISSNET databases,

including but not limited to RISSIntel and RISSGang, subject to all of the following conditions:

a. The submitting officer certifies that such information is in compliance with all applicable laws and regulations in the submitting agency's state pertaining to juveniles. *(As of the current effective date of this guideline, this criterion specifically excludes members from Missouri from utilizing the RISS criminal intelligence databases to submit or otherwise share information pertaining to juvenile suspects unless such activity is in compliance with applicable Missouri laws and regulations.)*

b. The submitted information involves felony-level, serious misdemeanor or gang-related criminal activity,

c. The submitted information is otherwise in compliance with MOCIC submission criteria and all applicable laws and regulations, including but not limited to 28 CFR Part 23, and

d. The information successfully passes the established MOCIC review procedures for database submissions as contained in MOCIC Member Guidelines for Intelligence Services (Intelligence Guidelines).

II. SUBMISSION PROCEDURES

A. Intelligence Submissions

As previously mentioned, the RISS intelligence database is comprised of members' timely, high-quality intelligence submissions. Therefore, we encourage you to submit information that meets 28 CFR Part 23 criteria on as many criminal suspects as possible.

MOCIC provides several ways for officers to submit intelligence. Officers may enter submissions directly from a remote connection or can submit the intelligence to MOCIC electronically via e-mail using the form available on the secure MOCIC home page. An electronic batch load submission process is also available.

Additionally, officers can submit their intelligence in written form, via mail, e-mail, fax or hand delivery, using an MOCIC RISSIntel Criminal Database Submission Form or a previously approved form, or via phone when submitted as part of an intelligence inquiry. Each of these procedures will be described and examples of the various forms and formats follow.

1. Electronic Submissions

The RISS Secure Cloud (RISSNET) is available to all RISS member agencies and allows RISS participants that are connected remotely to submit intelligence quickly and easily by logging on to RISSNET via the Internet. For database assistance in submitting your intelligence, contact the Intelligence Supervisor at (800) 846-6242, ext. 4140. For technical computer assistance related to your agency's remote connectivity, contact the MOCIC help desk at (800) 846-6242, option 5. Additional advice and assistance is available from your MOCIC Law Enforcement Coordinator (LEC).

a. Entering Data

(1) Users should **log on** to RISSNET following the procedures outlined in the network handbook provided to each agency. For help with this process, contact the MOCIC help desk number listed above.

(2) Users should **select the RISSIntel link** on the MOCIC home page or from the RISS Home Page (www.riss.net). The user should then select the "Search/Submit" tab to start the search/submission process. After making an inquiry, a new record can be added to the database. The submission process is initiated from the search results screen by selecting the "Add Submittal" button. You should fill in as much information as possible on the submission form. Remember, the reason officers submit information is to share it with other officers investigating the same individual or group, so share as much as possible.

(3) The RISSIntel submission screen is designed for quick entry of both regular criminal intelligence and the crime-specific **RISSGang** intelligence. If you want your gang intelligence labeled and stored in RISSGang, just click the RISS National Gang Database checkbox which is located near the top of the submittal screen. See page 4 for important information about RISSGang.

(4) The **RISSIntel** database captures information for each criminal "subject" based on the type of entity involved (suspect, organization, location, phone,

vehicle or weapon). The information requested is fairly standard for criminal justice databases and most fields are self-explanatory. A few fields are mandatory and those are designated in red for you. Many of the fields offer you a list of values or "pick list" from which to choose. This standardizes the data and assists you in data entry. A sample RISSIntel submission screen can be found in this guideline at **Appendix A.**

2. **Written Submissions**

Until remote access became available, member agencies traditionally submitted data on a written report form. MOCIC still accepts submissions in several written formats. The reports can be handwritten or typed and sent to MOCIC by mail, fax or e-mail, as well as hand-delivered, for entry into the RISS intelligence database. A brief description of the forms follows:

a. **MOCIC RISSIntel Criminal Database Submission Form**

MOCIC's standard report form is the MOCIC RISSIntel Criminal Database Submission Form. It is available to users by contacting MOCIC at (800) 846-6242. It is also available on the MOCIC home page under the Intelligence Resources heading. It captures many of the same fields as the electronic submission forms. Most of the fields are self-explanatory. The suspect (UNSUB - if name unknown), criminal activity, source and content reliability and 28 CFR Part 23 compliance fields are mandatory. Included on the form are several checkboxes to indicate whether you want the intelligence considered for *Digest* publication, posted on RISSLeads, or designated as RISSGang intelligence. Completing the form and appropriate checkboxes will expedite the data entry process. An example of the form and a description of its elements can be found at **Appendix B.**

b. **LEIN Forms**

(1) Four states in the MOCIC nine-state service region have adopted statewide **Law Enforcement Intelligence Network** (LEIN) programs that are coordinated by a state-level investigative agency. LEIN membership is comprised of municipal, county and other state law enforcement agencies within a respective state. LEIN member agencies submit intelligence through a state program, which is then available for dissemination to LEIN members. The state LEIN programs function as

intrastate information exchange mechanisms, while the RISS centers collectively serve as an interstate component of the evolving national criminal intelligence infrastructure.

LEIN intelligence submission forms in the states of Kansas, Nebraska, Iowa, and South Dakota have been deemed "previously approved" intelligence submission report forms for MOCIC/RISS.

(2) If the LEIN report form does not contain the following information, the top portion of an MOCIC RISSIntel Criminal Database Submission Form must be completed and attached to the LEIN submissions:

- Source Reliability (see **Appendix C**)
- Content Reliability (see **Appendix C)**
- RISSIntel Dissemination Code
- Verification of 28 CFR Part 23 Compliance

(3) LEIN intelligence submissions are submitted to MOCIC by the LEIN coordination agency and are processed in accordance with MOCIC guidelines.

(4) If a LEIN member agency is also an MOCIC member, any intelligence submission coming through LEIN will be processed and will identify the MOCIC member agency as the "submitting agency."

(5) If a LEIN member submits information to LEIN and is not an MOCIC member, the state agency that coordinates the LEIN program will be identified as the submitting agency when the submission is processed into the MOCIC/RISS system.

c. **Other Approved Forms**

(1) If a member agency prefers to submit intelligence to the RISS intelligence database using its own agency's intelligence report, it must submit a sample of the report form to MOCIC. The Intelligence Supervisor will determine if the report format is compatible with the MOCIC/RISS intelligence system and will advise the

agency if the form can be used in lieu of completing the MOCIC RISSIntel Criminal Database Submission Form.

(2) If an agency's intelligence report form is not fully compatible for submitting intelligence to the RISS intelligence database, it must be attached to an MOCIC RISSIntel Criminal Database Submission Form with the top boxed section completed, including the dissemination code, source and content reliability and submitting agency information.

3. **Batch Submissions**

To help agencies save time, MOCIC accepts intelligence submissions in an electronic format, which makes it much easier for those submissions to be included in the RISSIntel database. We call this process batch or bulk uploading. Many agencies already have data in some form of electronic database. Batching is designed to facilitate the data exchange in an easy manner.

Electronic data must be in a Comma Separated Value (CSV) format or other text delimited format. A simple submission form must be completed and included with the electronic data when sending it to MOCIC. This form provides the necessary information for each item in the batch submission that would have been provided for any regular submission to the MOCIC database. It is important to remember that all submissions must comply with 28 CFR Part 23 regulations and MOCIC policies. All records must identify the suspected criminal activity. Once the electronic data is received, an MOCIC computer programmer will run parsing routines, if needed, and prepare the data for our intelligence staff to run through the batch or bulk upload program.

Records related to juvenile subjects will be sorted prior to the upload process and batched in compliance with MOCIC policy.

Agency submissions will still be subject to MOCIC's standard quality control procedures and agencies will still receive notification of "hits" (see page 16) and other dissemination information, just like always. Once the process is completed, the agency's designated intelligence officer will receive a report, assuming, of course, that the designated officer has the necessary security control card on file with MOCIC. This report will advise how many records were successfully entered in the RISS system.

Each agency can set up a routine monthly or quarterly submission process. MOCIC recommends that agencies devise a system to flag those items in their database that have been sent to MOCIC to avoid confusion and/or duplicate submissions. Submitting criminal information into the RISSNET system can play a vital role in an agency's ability to participate in the important business of criminal information sharing. MOCIC stands ready to assist all our members. This new batch uploading functionality is intended to make information-sharing participation as easy as possible.

Additional batch instructions are located on MOCIC's home page or by contacting the Intelligence Supervisor at (800) 846-6242 (ext. 4140).

4. **Submissions Through Criminal Information Specialists**

Submissions may be made via MOCIC **Criminal Information Specialists** when their assistance is requested in locating additional intelligence. This section covers procedures for inputting information into the database based on information supplied during an inquiry. The inquiry process is discussed in Section V of this guideline.

a. Intelligence is normally returned to an agency when a request for assistance results in a Criminal Information Specialist locating a "hit" in the intelligence database or from another source. Information that a requesting agency supplies does not automatically go into the RISS intelligence database, as it may not necessarily meet the requirements of 28 CFR Part 23. Intelligence located from an inquiry is documented and returned to the officer making the request for information.

b. When information developed during an inquiry meets the requirements of 28 CFR Part 23, a member agency may request the information be entered into the RISS intelligence database. The procedures for entry are the same as regular written submissions, except for the following:

   (1) The Criminal Information Specialist determines if the information complies with 28 CFR Part 23 and enters the information into the database as a submission.

   (2) Intelligence staff members may review the entered submission for completeness and compliance based on the

information documented by the Criminal Information Specialist.

B. Dissemination of Database "Hits"

Incoming information will be checked against the MOCIC intelligence database as part of the submission process. Information that is determined to match or have a high probability of matching, also known as generating a "hit," will be disseminated in accordance with the MOCIC dissemination policy and instructions of the contributor.

C. Review Procedures

MOCIC has implemented a review procedure to assist submitting officers with 28 CFR Part 23 and MOCIC policy compliance. All intelligence submissions, both electronic and written, are subject to the following review procedures:

1. The Intelligence Specialist is responsible for reviewing incoming written submissions for completeness and compliance with 28 CFR Part 23 before assigning them to an Intelligence Clerk for entry. The Intelligence Specialist will double-check completed entries.

2. The RISSIntel electronic form contains a mandatory verification field in which the submitter certifies the information is in compliance with 28 CFR Part 23. The MOCIC RISSIntel Criminal Database Submission Form contains a check box certifying compliance with 28 CFR Part 23 and, if applicable, state juvenile information laws.

III. MOCIC INTELLIGENCE AUDITING AND PURGING CRITERIA

A. Purpose

28 CFR Part 23.20(h) mandates that MOCIC adopt procedures which will assure that ... *"all information (intelligence) which is retained...has relevancy and importance" and to "provide for the periodic review of information and the destruction of any information which is misleading, obsolete, or otherwise unreliable..."*

B. RISSIntel Record Footprint

A simple audit trail within the RISSIntel database is the visual "footprint" at the bottom of each RISSIntel submission; it lists officers who viewed a particular database record. Only authorized RISS members are able to

access the intelligence, and the "footprint," which includes the viewing date, officer's name, agency, state and phone number appears only on open dissemination records. This informal "footprint" is a way for the submitting officer to know which RISS members have viewed the information contained in the record.

C. Purging

An intelligence file shall be purged when any one of the following conditions is present:

1. The submitting member agency neither updates nor validates the information contained in the file and does not authorize its retention after five years.

2. Information in any RISS intelligence database file is found to be misleading, untrue or otherwise unreliable.

3. Information is determined to be irrelevant and/or no longer fully conforms to the RISS intelligence database input criteria or MOCIC policy.

4. Information in the file no longer conforms to the provisions of 28 CFR Part 23.

5. When the submitting agency requests the information be purged.

6. If the submitting agency terminates its MOCIC membership.

D. Retention

1. Retention Period

   Intelligence submissions will be retained in the RISS intelligence database for a five (5) year period unless the submitting officer requests a shorter retention period or earlier deletion.

2. An intelligence file can be retained in the RISS intelligence database for an additional five years if **both** of the following conditions are met:

   a. All information in the file fully conforms to the provisions of 28 CFR Part 23.
   b. All information in the file fully conforms to RISS intelligence database input criteria and MOCIC policy.

3. Retention can be accomplished in two ways:

a The retention is authorized by the submitting agency that, as owner of the information, has responsibility for its continued inclusion in the database; **OR**

b. When the submitting officer updates his record with a new criminal activity.

E. Disposition of Purged Information

Information purged from the RISS intelligence database shall be electronically eliminated by the computer system after purge date confirmation. Submitting agencies **will not** be notified of any pending intelligence purge. It is incumbent on the submitting agency to track its submissions. Contact a Criminal Information Specialist or the Intelligence Supervisor if the intelligence needs to be validated and the purge date updated for another five (5) year period.

IV. SECURITY and DISSEMINATION

MOCIC and the other RISS centers take information security very seriously. The safety of law enforcement officers often lies in protecting information. Therefore, MOCIC has adopted very strict dissemination procedures to ensure the integrity of the submitted information and the security of those who share information via MOCIC/RISS information systems.

A. Identity Validation

MOCIC requires all users of intelligence services to complete the **RISS Online Registration process.** User access must be approved by the Administrative Head, Executive or Agency Representative, and the registration must include requested information that allows MOCIC staff to verify the identity of those contacting us. The link to RISS Online Registration can also be obtained from your MOCIC Law Enforcement Coordinator (LEC) or by calling the Membership Support Coordinator at (800) 846-6242, ext. 4108.

B. Need-To-Know/Right-to-Know

The right-to-know and need-to-know principles are used to determine whether an officer making an inquiry or otherwise requesting information is authorized to receive it. These terms can be confusing. Right-to-know implies that the individual is in a legitimate law enforcement role and in good standing within his/her agency. Right-to-know is similar to holding a security clearance that allows you potential access to law enforcement intelligence. Need-to-know is determined by the agency responsible for the information or, in other words, by its owner. The owner of information

submitted to the RISS intelligence database always determines need-to-know through the dissemination code assigned. Right-to-know is determined by the user's agency administration and means:

1. You are an employee of an MOCIC member agency/other RISS center or a vetted, non-RISS law enforcement member, **and**,

2. You have been properly authorized through the RISS Online Registration process and have been designated by your department as an access officer for MOCIC/RISS services.

C. Dissemination

All data submitted to the RISS intelligence database by member agencies must contain a dissemination code. Submission forms received at MOCIC with no designated dissemination code will be considered "open". This code immediately notifies the online inquirer or MOCIC staff member how the owner of the information wants dissemination handled.

MOCIC will **only** release information in accordance with the submitting agency's dissemination code. Whenever intelligence is disseminated as a result of an inquiry, the submitting agency will be notified about the dissemination by e-mail, telephone or fax. Once the requestor's identity has been validated, either by the security information contained in MOCIC membership records or SSL certificate used with the Internet browser, the selected dissemination code determines the amount of information to be released. There are three dissemination codes associated with the RISS intelligence database.

- Open – Release All Information
- Release Limited Information
- Restricted – No Information Released

1. "Open-Release All Information"

   a. This indicates that information submitted may be disseminated to any authorized RISS member agency officer, MOCIC or another RISS center checking on a suspect or event in the information.

   b. Information may be published in the MOCIC *Criminal Information Digest – Online.*

2. "Release Limited Information"

a. When this code is used, the staff of MOCIC or other RISS centers will disseminate only limited information.

b. This dissemination code dictates that limited identifying information is released to the inquiring agency along with the name of the contributing agency, the MOCIC member contact, and the telephone number.

3. "Restricted – No Information Released"

a. **MOCIC does not recommend this option** because it creates "blind" hits.

b. Using this dissemination code is so restrictive that an inquiring officer will not be immediately alerted that information exists in the RISS database. MOCIC intelligence staff receives the restrictive notification then contacts the submitting officer for approval to release intelligence contact information.

4. The only exception to this policy will be in accordance with 28 CFR Part 23.20 (f) (2), which provides for the dissemination of an assessment of criminal intelligence to a government official or to any other individual when necessary to avoid **imminent danger to life or property**. If these conditions are met, the submitting agency shall be immediately notified of the circumstances leading to any deviation from established dissemination instructions.

V. ASSISTANCE IN LOCATING ADDITIONAL INFORMATION (INQUIRY)

A. Requests for Assistance

MOCIC members may request assistance through the Criminal Information Specialists in locating additional information from sources available to MOCIC. To access this service, a member must have the appropriate security information in MOCIC membership records. A request for assistance may be made by an authorized officer via telephone, e-mail, fax, or in person.

B. Criteria for Requests

1. Information supplied during an inquiry request (if compliant with 28 CFR Part 23) can be maintained in the RISS intelligence database for a period of five years as a submission. Officers are urged to request this service.

2. All information contained in the RISS intelligence database is the property of the submitting agency and will be disseminated only in accordance with dissemination instructions provided by the submitting agency. Other CJI information will be submitted in accordance with applicable security policies.

3. Information, in whatever form, will be disseminated only to authorized RISS users.

4. Information shall be disseminated only to persons who meet the need-to-know/right-to-know criteria and who have been granted necessary permission to access RISS intelligence.

5. Information will only be disseminated for a legitimate law enforcement purpose. This requirement is satisfied if the person making the inquiry identifies the type of suspected criminal activity or other purpose that generated the inquiry.

C. Types of Requests

Requests for assistance may be made to MOCIC for the following:

1. Searches for criminal information on individuals, groups, organizations, gangs or businesses, weapons, locations, vehicles and phone numbers.

2. Special requests that involve the collation and/or analysis of several MOCIC intelligence files or other data.

3. Other information requests where the results will assist the member officer in accomplishing a legitimate law enforcement purpose.

D. Procedure for Requesting Information Assistance

1. Requests may be made by phone, fax, mail, in person or by e-mail via the RISS secure intranet. A portion of the Online Inquiry Form can be found at **Appendix D**.

3. To make a request by telephone, call MOCIC Criminal Information Specialists at (800) 846-6242 (option 2). Email requests to inquiry@mocic.riss.net.

4. To make a request for information assistance, MOCIC requires a minimum of:

    a. Case number

    b. Type of criminal activity or other circumstances that generated the request for assistance.

    c. Descriptors about the criminal suspect, gang, business, organization or other entity.

4. If available, the following information should be given to MOCIC:

    a. Suspect's Social Security Number

    b. Suspect's date of birth

    c. Suspect's physical description

    d. Other identifying data for the suspect (i.e., driver's license state and number, tattoos, scars, etc.)

    e. Geographic areas where the suspect is thought to be involved in criminal activity or any specific areas the inquiring agency would like checked.

E. Information Sought in Response to Information Assistance Requests

1. The RISS intelligence database is checked in response to all requests for assistance made to the Criminal Information Specialists. Other law enforcement or commercial databases may be used in compliance with any applicable database security policies if the request meets MOCIC's internally-specified requirements.

2. MOCIC will not disseminate any criminal history information obtained from these authorized databases. Authorized members may be encouraged to conduct a criminal history check on their own.

3. As required, MOCIC will contact or place the member in contact with other law enforcement agencies that might have additional related information beyond that in the RISS intelligence database.

4. If the subject of the request is suspected of involvement in criminal activity outside the MOCIC service region or if there is an indication intelligence might be available from law enforcement agencies outside the MOCIC service region, MOCIC may contact other RISS

centers for assistance with the request. The other RISS centers will contact members in their service region to facilitate contact with the MOCIC member regarding the request.

5. Driver's license photo assistance may be available in accordance with applicable state laws, regulations and guidelines.

F. Inter-RISS Center Inquiry Assistance

MOCIC will frequently, and upon special request, seek assistance from and offer assistance to the other RISS centers. The other five RISS centers and their service regions are as follows:

1. **Western States Information Network® (WSIN)**
   Washington, Oregon, California, Alaska, Hawaii, Canada, and Guam

2. **Rocky Mountain Information Network® (RMIN)**
   Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, Wyoming and Canada

3. **Regional Organized Crime Information Center® (ROCIC)**
   Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia, U.S. Virgin Islands and Puerto Rico

4. **Mid-Atlantic/Great Lakes Organized Crime Law Enforcement Network® (MAGLOCLEN)**
   Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, District of Columbia, Canada, England, and Australia

5. **New England State Police Information Network® (NESPIN)**
   Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont and Canada

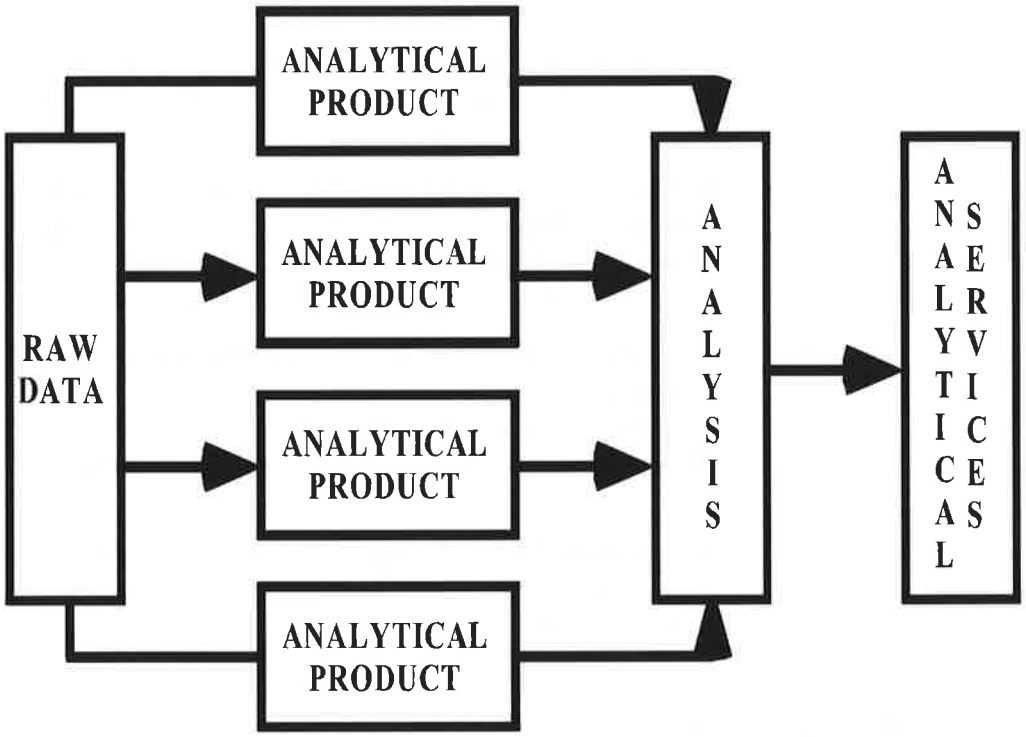
VI. MOCIC ANALYTICAL SERVICES

Another service provided by MOCIC is the analysis of complex intelligence and/or investigative data regarding criminals, organizations, groups, businesses and/or criminal activity. The objective of this service is to convert raw, disorganized, unfinished information into "focused" or finished intelligence. To provide this service, MOCIC staff includes a complement of intelligence analysts who are highly trained and experienced in the field of intelligence analysis. The analysts use a variety of techniques, some manual and some with computerized graphic and data-management programs developed specifically to provide this service. This section describes the various analytical services available through MOCIC and defines the types of analytical products normally developed in the course of

providing these services and identifies the procedures for requesting analytical services.

A. Intelligence Analysis

Intelligence analysis is the heart of an intelligence system. During analysis, assembled bits and pieces of raw information collected from many different sources are collated (organized) in a manner to show pattern and meaning. Without this analysis, no interpretation or additional meaning can be derived from this collected information. Many times, analytical *products* are confused with a complete analytical *service*. An analytical product, such as a link chart or flow chart, is not a completed analysis, but is one of the components or building blocks used in the construction and dissemination of an analytical service. This is illustrated in the following diagram:



B. Definitions

1. Analytical Service

The manual and/or automated method of research, compilation, interpretation and presentation of investigative data and/or intelligence on a felony case for MOCIC member agencies.

2. Analytical Product

A written report, briefing, graph, chart, and/or computer listing resulting from the compilation and interpretation of raw information, prepared in response to a member agency's request for an analytical service (that relates to felony-level criminal activity).

C. Types of Analytical Services

1. Case Analysis

The compiling and combining of investigative data and/or intelligence reports that are collected in a specific criminal investigation.

The objective of the case analysis is to identify criminal activity and associations that are then disseminated in an intelligence report. Analytical products normally developed during a case analysis include link analysis charts, commodity flow charts, cash flow charts, event flow charts, time line charts, summary reports and recommendations. Case analyses are very useful in analyzing conspiracies, complex criminal operations or the results of any proactive law enforcement operation.

2. Financial Analysis

The compilation, review and interpretation of financial documents, records and/or transactions to reconstruct financial activities pertaining to individuals, organizations, groups or businesses suspected of being engaged in criminal activity.

Analytical products normally constructed during a financial analysis include reports, specialized graphics, or spreadsheets depicting a series of complex financial transactions.

3. Criminal Activity Analysis

The compilation and interpretation of information from a variety of sources, such as publications, intelligence databases, reports submitted by MOCIC member agencies, etc., aimed at developing comprehensive and reliable information to assess a specific criminal activity or crime group.

Analytical products that might be developed during the course of a criminal activity analysis include link analysis charts, various types

of flow charts, time line charts, assessment reports or special criminal identification reports.

4. Telephone Traffic Analysis

The evaluation and interpretation of the telephone traffic of entities suspected of being engaged in some form of criminal conduct. The analysis results are provided in the form of charts, summary reports, briefings, recommendations, and/or computer listings (products).

Telephone traffic analysis is a specialized analytical service and, as a result of the analysis, MOCIC staff members develop various products that are unique to telephone traffic analysis. A brief summary of the specialized analytical products is provided later in this guideline.

For a telephone traffic analysis, records of telephone calls must be submitted in **electronic format** other than a .pdf file. An acceptable electronic format would be a comma delimited or tab delimited format. MS Excel files are preferred. These records can be any combination of pen-register records, records obtained from legally authorized wiretaps, telephone bills listing local and/or long-distance phone calls, telephone company records normally supplied by subpoena, and/or any other type of record which lists individual telephone traffic among a group of telephone numbers. Telephone traffic analysis can be extremely valuable when dealing with complex conspiracy investigations. Telephone records should be subpoenaed in an **electronic format** to avoid manual data entry.

D. Types of Analytical Products

1. Assessment Report

A comprehensive report containing the findings, conclusions and/or recommendations of the MOCIC analyst, derived from the study, research and analysis of available information for the purpose of determining general criminal activity.

2. Special Identification Report

A compilation of physical identifiers, modus operandi, data, and/or other identifying or background data of all known suspects engaged in a particular criminal activity or members/associates of a particular group.

Special identification reports generally contain comprehensive information on the pertinent suspects, but include no formal assessment of trends or patterns.

3. **Link Analysis Chart**

A graphic representation of known and suspected associations among individuals, businesses, organizations, telephone numbers, groups, etc., suspected of being involved in criminal activity.

4. **Flow Chart**

A graphic representation of the direction or flow of commodities, money, information and/or events involved in criminal activity.

Types of flow charts include:

a. **Event Flow Chart**

A chronological flow of events in a particular criminal activity.

The event flow chart stresses both the sequence (order in which events occurred) and dependency (what event occurred as a result of a prior event).

b. **Commodity Flow Chart**

A chart tracing the flow of some commodity (i.e., narcotics, stolen cars, etc.) in a particular criminal conspiracy or activity.

Commodity flow charts are particularly valuable in establishing the hierarchy of large-scale criminal operations. They are one of the most commonly constructed analytical products in narcotics investigations.

c. **Cash Flow Chart**

A chart tracing the flow of money as it moves through a criminal organization(s).

It is particularly useful in identifying and defining the role of management levels within a criminal organization(s).

5. **Time Lines**

A comprehensive form of event flow charting useful both in intelligence analysis and as a case management tool.

Time line charts summarize investigative actions, as well as activities of suspects, victims and witnesses. Like other forms of flow charting, these charts can be the product of several types of analytical services. They are normally a much more detailed type of chart, breaking activities into small components.

6. **Criminal Activity Summary Report**

A written synopsis of the pertinent elements of information relative to criminal suspects, activities, telephone traffic records and/or financial records developed from a case under analysis.

7. **Briefing**

A verbal presentation to member law enforcement personnel of the key elements of criminal activity and subject data resulting from a case under analysis.

8. **Collection Plan/Survey**

A guide for use in collecting information pertaining to a specific criminal activity, group or individual to provide the MOCIC analytical staff with data for analyzing the scope or extent of the problem, or to provide investigators with leads for further investigations.

9. **Computer Listing**

Automated reports derived from computer programs designed to compile and sort large amounts of case data, financial data, telephone traffic data, intelligence and/or criminal activity data that are then used to aid analysis and interpretation of information and to develop charts, recommendations, or other reports or briefings.

10. **Telephone Traffic Analysis Analytical Products**

There are several analytical products normally developed and disseminated to member agencies during a telephone traffic analysis. These products are unique in that they pertain only to telephone traffic and include:

a. Chronology Reports

b. Frequency Reports

c. Common Call Reports

d. Special Reports – Custom Design Combination of a-c

E. Procedures for Requesting Analytical Services

1. Requests for analytical services may be submitted by telephone, e-mail, fax, in writing or in person. Requests should include the following information:

   a. Type of felony-level criminal activity

   b. Scope of the criminal activity (how large or widespread)

   c. Jurisdictions or geographic area involved

   d. Other law enforcement agencies involved in the investigation

   e. Type of analytical services and products desired (if known)

2. **Do not send materials until MOCIC has accepted your case.** Avoid sending original evidence. Avoid sending original reports or original/only copy photographs. MOCIC will not photocopy large volumes of material for the submitting agency.

F. Submission of Data for Analytical Services

1. Bulk intelligence and/or investigative data submitted for analysis is not processed into the RISS intelligence database. However, in instances where there is reasonable suspicion of criminal activity, intelligence will be entered in the appropriate RISS intelligence database with approval of the contributing agency. **In most cases, an intelligence submission is required before MOCIC will accept a case for analysis.**

2. Bulk intelligence and/or investigative data for analysis does not have to conform to the MOCIC input criteria (see Section I), however, there must be suspected felony criminal activity.

G. Disposition of Data

At the conclusion of an analytical service, intelligence and/or investigative data submitted by the requesting agency and all analytical products developed during the analytical service are returned to the submitting agency. Original material can be shredded upon request.

H. Security

1. Access to data submitted for analysis is limited to the MOCIC analyst staff, necessary clerical support personnel and MOCIC management.

2. MOCIC does not disseminate data submitted for analysis except to the contributor unless they have given further direction.

VII. DIGITAL FORENSICS

MOCIC provides digital forensics services to its member agencies to assist in all phases of criminal investigations. MOCIC's experienced digital forensic staff provides these services, which include data recovery, computer media copying, evidence exams, search and seizure assistance, date and time stamping information, unallocated disk space search and evidence documentation.

A. Types of Digital Forensics Services

1. **Data Recovery**
   MOCIC has the ability to attempt recovery of computer files that have been deleted, encrypted or hidden on a personal computer.

2. **Computer Media Copying**
   MOCIC staff can make forensic copies of electronic, magnetic and optical computer storage media for further examination.

3. **Search and Seizure Assistance**
   Your agency can obtain informational assistance regarding the search and seizure of computer-related evidence.

4. **Date and Time Stamping Information**
   MOCIC can examine computer files and provide reported date and time information regarding file creation and modification.

5. **Unallocated Disk Space Search**

MOCIC computer forensic staff can conduct a search of all unallocated hard disk space to look for residual information that might be used as evidence.

6. **Evidence Documentation**
Printed and electronic copies of evidence found on the examined media can be provided to the requesting member agency.

7. **Handheld Device Forensics**
MOCIC can perform analysis on many types of handheld devices including personal digital assistants (PDA's), cell phones, and GPS devices. MOCIC may be able to extract phonebook information, call history, text messages, photos, videos, and other information contained on these devices.

B. Procedures for Requesting Digital Forensics Services

1. Requests for digital forensic services should be made by contacting one of the digital forensics examiners at 800-846-6242 ext. 4223.

2. The Analytical Supervisor will review all requests to ensure that the following criteria are met:

   a. The requesting agency must be a member of MOCIC.

   b. The request must identify the criminal activity being investigated.

   c. There must be a reasonable suspicion that the criminal activity is felony-level and multijurisdictional.

   d. Businesses and organizations submitted must be considered involved in the criminal activity or exist for the purpose of criminal activity.

   e. The computer (including handheld devices) and all the components of the computer must have been legally seized. In most cases, MOCIC will limit its services to seizures based on a valid search warrant.

   f. The targets of the investigation must be submitted to the RISS intelligence database, if 28 CFR Part 23 requirements are met.

3. If the request for forensic services is approved, MOCIC's digital forensic staff will conduct an interview with the requesting agency case representative. The digital forensic staff will ensure that copies of the search warrant or consent are included with the questionnaire form. **Do not send devices or software to MOCIC until your request has been approved and you are contacted and asked to send the hardware.**

C. Disposition of Evidence

At the conclusion of all examinations, the Computer Forensics Analyst will present all potential evidence to the agency case representative. MOCIC does not retain copies of reports or evidence.

D. Security

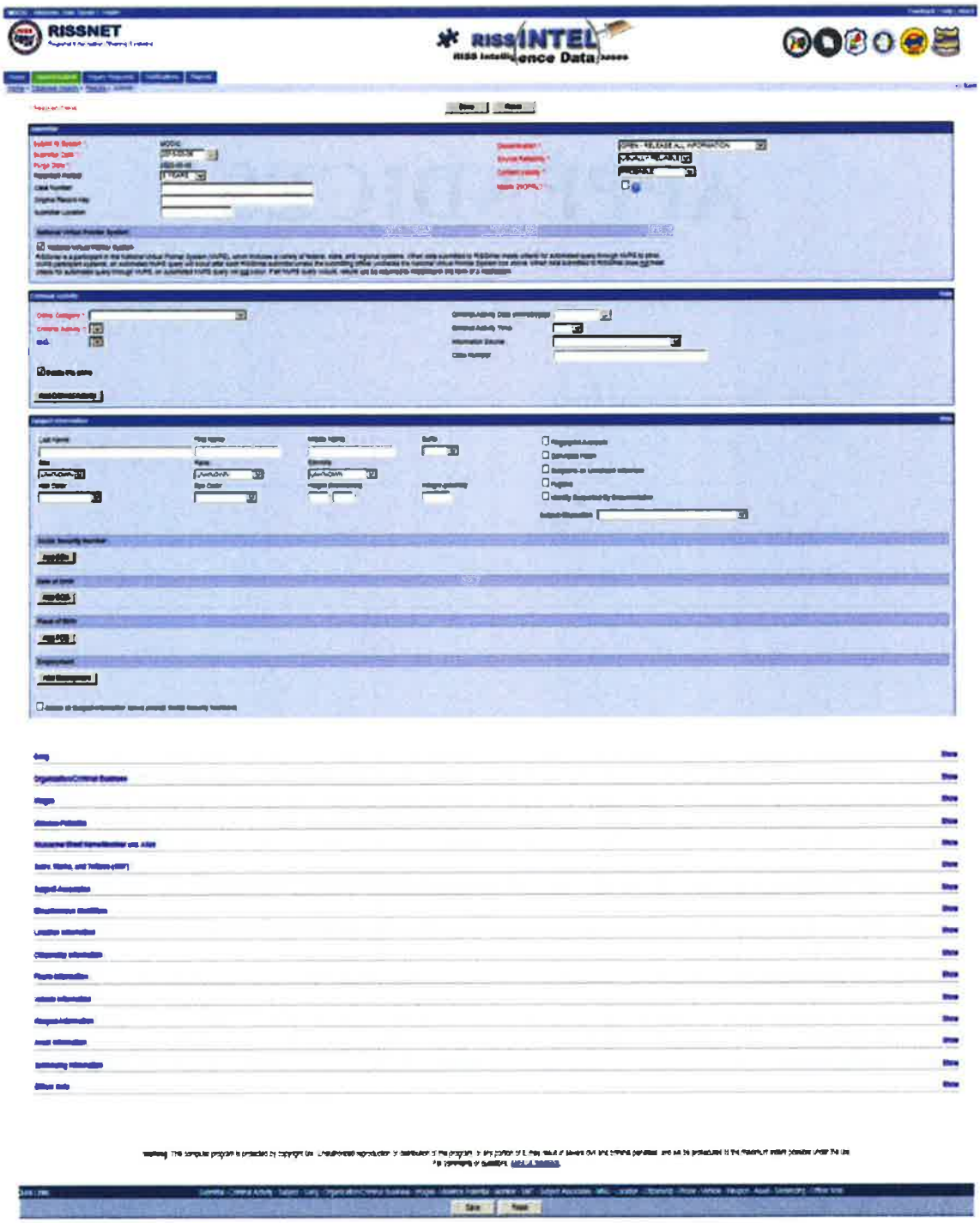
Access to the computer and related components submitted for examination is limited to the Computer Forensics Analyst and MOCIC Management.

This document was prepared under the leadership, guidance and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice in collaboration with the Mid-States Organized Crime Information Center. 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.

APPENDICES

Appendix A

RISSIntel Submission Screen



Mid-States Organized Crime Information Center
RISSIntel CRIMINAL DATABASE SUBMISSION FORM

Mail or Fax to: MOCIC
P.O. Box 1250
Springfield, MO 65801-1250
Fax: (417) 883-1532

(Information in Bold Type Within the Dotted Line Must Be Completed. If Additional Space Is Needed For Any Item, Please Use The Reverse Side Of Form)

Agency State: _____ **Agency Name:** _____ **Agency #:** _____

Submitting Officer Name: _____ **Phone:(____)** _____

☐ **I certify this submission meets the requirements of 28 CFR Part 23** **Case #:** _____

☐ **If this suspect is a juvenile, I certify this information has been provided in compliance with my state's applicable laws and regulations**

Dissemination: ☐ **Open (Consider for Publication)** ☐ **Open** ☐ **Release Limited Information**

Source Reliability: ☐ **Reliable** ☐ **Usually Reliable** ☐ **Unreliable** ☐ **Unknown**

Content Reliability: ☐ **Confirmed** ☐ **Probable** ☐ **Doubtful** ☐ **Cannot Be Judged**

Post on RISSLeads? ☐ YES ☐ NO (For Gang Info. Only) Enter in RISSGang?** ☐ YES ☐ NO

**By checking the "Yes" box, you understand and agree that the information you submit to the RISS National Gang Database (RISSGang) portion of RISSIntel can be available to all law enforcement and criminal justice agency professionals, including non-RISS members, who have been identified, vetted and given access to RISSGang.

Criminal Activity **Brief description of suspected criminal activity (Use reverse side of form if necessary):** ☐ **Narrative attached**

SUSPECT INFORMATION

Last Name: _____ **First Name:** _____ **Middle Name:** _____ **Suffix:** _____

Sex: ☐Male ☐Female **Race:** ☐American Indian ☐Asian ☐Black ☐Hispanic ☐White ☐Unknown

Hair: _____ **Eyes:** _____ **Height:** _____ **Weight:** _____ **Violence Potential:** ☐Yes ☐No ☐Unknown

Check all that apply: ☐U.S. Citizen ☐Fingerprints Available ☐Convicted Felon ☐Subject Is Unreliable Informant

DOB: ___/___/___ **DOB:** ___/___/___ **SSN:** ___-___-___ **SSN:** ___-___-___

AKAs: _____

Residence Address: _____ **Residence Phone:** _____

City: _____ **State:** _____ **Zip:** _____ **Occupation:** _____

SCARS/MARKS/TATTOOS

S M T Body Location/Description: _____

CRIMINAL ASSOCIATES

(**Please Note: Associate(s) listed below should also be submitted on separate criminal database submission forms.**)

Name: _____ **DOB (mm/dd/yy)** _____ ☐ Same Criminal Activity

Name: _____ **DOB (mm/dd/yy)** _____ ☐ Same Criminal Activity

CRIMINAL ORGANIZATION/GANG/BUSINESS

Name: _____

Type: (ie: street gang, business, etc.) _____ **Business Address:** _____

Business Phone: _____ **City:** _____ **State:** _____ **Zip:** _____

MISCELLANEOUS NUMBERS

Driver's License: (include state) _____

SID: (include state) _____ **FBI Number:** _____

Other Miscellaneous Numbers: _____

VEHICLE INFORMATION

Type: (ie: auto, truck, etc.) _____ **Style:** _____

Year: _____ **Make:** _____ **Model:** _____ **Color:** _____

License #: (include state) _____ **VIN #:** _____ **Descriptive Features:** _____

FOR MOCIC USE ONLY: **Date Received:** _____ **MOCIC #:** _____

Date Entered: _____ **By:** _____

Revised 11/08

DESCRIPTION
MOCIC RISSINTEL CRIMINAL DATABASE SUBMISSION FORM

I. Top Section

A. Submitting Agency Information

The top section of the submission form is self-explanatory. However it is very important that all information be completed, including your member agency number, as well as state, telephone, etc. The name of the person submitting the report is essential.

B. Dissemination Code

Check the appropriate box to indicate the level of dissemination you wish assigned to the submission (Open-Consider for Publication, Open or Release-Limited dissemination). All intelligence submissions must contain a dissemination code. **Submission forms received at MOCIC with no dissemination code marked are considered to be Open dissemination.**

C. Data Evaluation

Use these sections to evaluate the Source Reliability and Content Reliability of the information. If further information is desired on the data evaluation, please refer to **Appendix C.** Submission forms received at MOCIC with no reliability marked are considered to be "usually reliable and probable" – which are the database default settings.

D. Additional Intelligence Instructions

Use the checkboxes to clearly indicate if you want the intelligence included in RISSGang or posted on RISSLeads bulletin board. Other checkboxes are available to indicate submission meets 28 CFR Part 23 and if applicable, state juvenile information laws.

E. Brief Description of Suspected Criminal Activity

This is the narrative portion of the report, and it is very important that this section be completed or that a narrative is attached. The submitting agency must describe the circumstances resulting in a reasonable suspicion that the subject of the report is involved in the requisite criminal activity. This block should indicate specific

criminal activity, the subject's level of involvement and the geographic area(s) where the activity and/or the impact of the activity occur.

II. Bottom Section

A. Identifying Data (self-explanatory)

B. Violence Potential

Check the "yes" block if the subject has any history or tendency toward violence; i.e., armed and dangerous, carrying a concealed weapon, assault on a police officer, violent offender, etc.

C. Criminal Associates

Additional criminal subjects may be listed in this portion. Criminal associates can be included in RISSIntel database if DOB and criminal activity are provided. If the subject(s) listed here are involved in the same criminal activity as the main subject of the submission, check the box for same criminal activity. When possible, criminal associates should also be submitted on a separate form. Criminal associates must also meet 28 CFR Part 23 requirements.

D. Criminal Organization/Gang/Business

Use this section to list/describe any association the subject(s) of the submission might have with businesses that are:

1. Criminal in nature

2. Used to commit and/or facilitate criminal activity

3. Fictitious and used to commit criminal activity

Do not use place of employment unless it is suspected of being involved in crime.

E. Vehicle Information

Use this section to list any vehicle(s) to which the subject of the intelligence submission has access. If there is more than one vehicle, a notation of "see reverse side" may be made in this

section of the report with a list of the vehicles provided on the reverse side of the form.

III. Questions

Any questions on completion of the RISSIntel Criminal Database Submission Form may be directed to an MOCIC Criminal Information Specialist (option 2) or the Intelligence Supervisor (ext. 4140) at (800) 846-6242.

RELIABILITY EVALUATION OF SUBMITTED INFORMATION

Both written and electronic submission formats must be evaluated using source reliability and content reliability criteria prior to entry into the RISS intelligence database.

A. SOURCE RELIABILITY (Evaluation of Source)
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:

1. Reliable
   The reliability of the source is unquestioned or has been well-tested in the past.

2. Usually Reliable
   The reliability of the source can usually be relied upon. The majority of the information provided in the past has proven to be reliable.

3. Unreliable
   The reliability of the source has been sporadic in the past.

4. Unknown
   The reliability of the source cannot be judged. Authenticity of trustworthiness has not yet been determined by either experience or investigation.

B. CONTENT RELIABILITY (Evaluation of Information)
The reliability of information is an index of the accuracy of the information. The reliability of the information shall be assessed as follows:

1. Confirmed
   The information has been corroborated by an investigator or another reliable independent source.

2. Probable
   The information is consistent with past accounts.

3. Doubtful
   The information is inconsistent with past accounts.

4. Cannot Be Judged
   The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

Appendix D

Online Inquiry Form

MOCIC Criminal Information Specialists are available to assist you during normal business hours by dialing the Center at (800) 846-6242 and pressing Option "4". Please provide all available information to expedite this inquiry. **NOTE:** By submitting this form, you will not be checking the Intelligence Databases in a real time mode.

Section A

Last Name: First Name: MI:

Alias:

DOB: Race:

Sex:

○ Male

○ Female

Height: Weight: Eyes: Hair:

SSN: FBI#: SID# (list state):

DL# (list state):

Other Identifying Data (example: tattoos, scars, fingerprint classification, additional identifying numbers, etc.):

Residence Address:

VEHICLE INFORMATION

Year/Type: Make: Model:

Color: LIC#:

Click Here if you have multiple suspects.

28 CFR PART 23

Executive Order 12291
These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act
These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act
There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23
Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:
PART 23--CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec.

1. Purpose.
2. Background.
3. Applicability.
4. Operating principles.
5. Funding guidelines.
6. 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 Policy.

The mission of the MOCIC Equipment Services Unit is to provide member agencies with state-of-the-art surveillance equipment that will assist in gathering evidence in a timely and efficient manner. We also provide technical assistance and training, enabling members to properly utilize equipment at their disposal.

(800) 846-6242
Extension 4221

Please contact a member of the MOCIC Equipment Services Unit if you have technical or equipment questions, or need to utilize one of our many services.

Dan Woolman - Equipment Technician
dwoolman@mocic.riss.net

Brad Blades - Computer Info Specialist
bblades@mocic.riss.net

Virginia Netzer - Equipment Clerk
vnetzer@mocic.riss.net

Mid-States Organized Crime Information Center
P.O. Box 1250
Springfield, MO
65801-1250

A Proven Resource for Law Enforcement™

www.riss.net

MOCIC

Mid-States Organized Crime Information Center®

Equipment Services Unit

MOCIC

Mid-States Organized Crime Information Center

Equipment

Video recording systems

On-the-body video and audio recording systems

Body wire audio transmitter and receiver systems

GPS tracking equipment (both real-time and data logger units)

Pole cameras

Secure radio units (hand-held and vehicle-based units)

Digital SLR cameras

Monocular night vision scopes

Stabilized binoculars

License plate capture cameras

Car key FOB micro audio/video recorders

MOCIC Equipment Services

Loan technical surveillance equipment for use in conducting investigations

Provide technical assistance and advice in the deployment of technical surveillance

Perform complex filtering of audio recordings to clarify conversations

Research available equipment for agencies desiring to purchase surveillance equipment to meet specific needs

Perform video capture and image clarification from surveillance video

Construct pole cameras, antennas and microphones for purchase by member agencies

Accomplish minor repair of agency-owned surveillance equipment

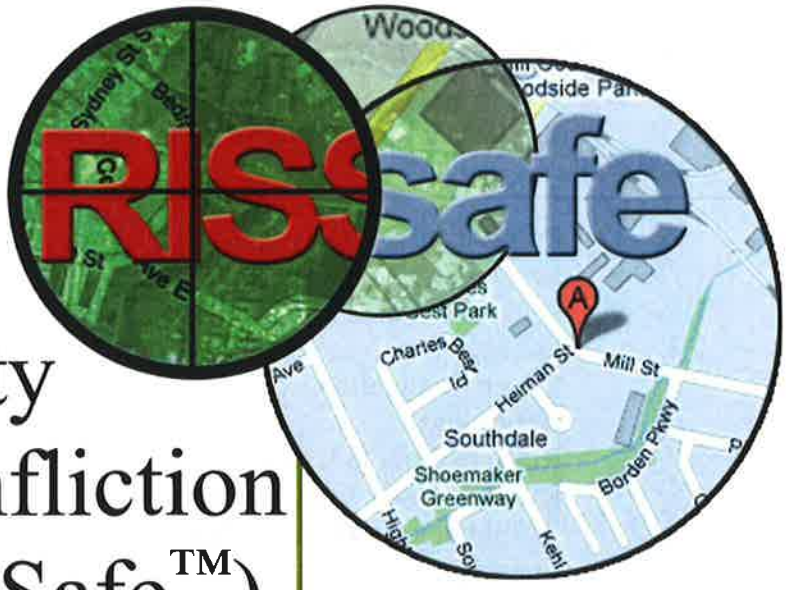
Training

Practical Applications of Surveillance Equipment (PASE)

The MOCIC Equipment Services Unit conducts a three-day class covering the basic theory and use of technical surveillance equipment.

For more information about the PASE, or to register to take the class, go to the MOCIC Web Site and click on the Training Announcements Link.

MOCIC P.O. Box 1250, Springfield, MO 65801-1250 (800) 846-6242, extension 4221



RISS Officer Safety Event Deconfliction System (RISSafe™) Policy

August 2018

Regional Information Sharing Systems®

Table of Contents

Section ***Page***

Appendices

Approval Date: October 7, 2008	Effective Date: October 7, 2008
Revision Date: November 2008, January 2009, February 2009, March 2009, June 2009, July 2009, May 2010, October 2010, February 2011, February 2012, April 2013, February 2014, March 2015, May 2015, August 2015, April 2016, August 2018	

Regional Information Sharing Systems (RISS) Officer Safety Event Deconfliction System (RISSafe) Policy

1. Purpose

The Regional Information Sharing Systems (RISS) Program recognizes and has included in its mission the goal of promoting officer safety. RISS developed RISSafe as an officer safety event deconfliction system in furtherance of this goal. Because of the operational and officer safety issues related to an event deconfliction system, specific policies must be established to ensure that operational guidelines are in place to provide consistent, appropriate, and effective use of RISSafe.

An agency other than RISS that acts as a RISSafe Watch Center or participant may, for agency use, develop a more restrictive version of this policy that is consistent with the agency's mission. Agencies acting as a RISSafe Watch Center agree to provide a copy of their policy to RISS. Software recommendations and changes may be considered on a case-by-case basis and will be implemented, if approved by the RISS National Policy Group (RNPG). RISSafe Watch Centers and participants agree to comply with other applicable RISS policies, as well as their own policies, in areas such as electronic communications, security, information sharing, and privacy.

2. Scope

This policy applies to all RISSafe users. RISSafe is available for use by personnel from law enforcement agencies. Users shall adhere to the current version of this policy.

3. Authority

The RNPG provides for the oversight of RISSafe, the RISSafe Policy, and related programs. The RISSafe Program Advisory Group considers software enhancements and changes to RISSafe for eventual recommendation to the RNPG.

4. Preface

RISSafe is an officer safety event deconfliction system. Often, investigative efforts, such as undercover operations, create a situation in which agency personnel work in close proximity to each other. In other situations, agencies or officers may be investigating the same subject at the same time. In either case, agencies or officers may interfere with each other's investigations, causing investigative efforts to be disrupted or, worse, officers or citizens to be unintentionally hurt or killed. RISSafe stores and maintains data on planned law enforcement events submitted for inclusion (e.g., raids, controlled buys, surveillances), as well as appropriate noninvestigative events, with the goal of identifying and alerting affected agencies or officers of potential conflicts impacting law enforcement efforts. The use of an officer safety event deconfliction system allows for controlled and secure monitoring of these operations and the immediate notification of affected parties when potential conflicts arise. RISSafe works in conjunction with the RISS Criminal Intelligence Database (RISSIntel™) to provide additional information and target deconfliction.

5. System Integration

There are three nationally recognized event deconfliction systems—RISSafe (used by RISS members, fusion centers, some High Intensity Drug Trafficking Areas [HIDTAs], and other appropriate entities), Case Explorer (used by some HIDTAs), and SAFETNet (used by some HIDTAs).

In May 2015, the three systems were connected using an interface solution known as the Partner Deconfliction Interface (PDI), which was developed in coordination with the system owners. The PDI serves as a pointer (or system-to-system) solution. When a submission is made into one of the systems, the PDI enables a query against the two other systems. If a conflict is identified, information regarding that conflict is returned. Notifications are made to the affected officers. (*Note: Work continues to integrate New York.*)

6. Definitions

Area of Interest (AOI) – A geographic area monitored by a RISSafe Watch Center consisting of one or more counties. Only RISS may define an AOI, and only the RISS Technology Support Center staff can establish an AOI within RISSafe.

RISSafe Remote Users – Those individuals connected via the RISS Secure Cloud (RISSNET™) who are provided permissions to RISSafe and who may submit an event directly to RISSafe without the intervention of a RISSafe Watch Center.

RISSafe Watch Center – A law enforcement center (such as a RISS Center, a fusion center, a HIDTA, or a state law enforcement agency) that operates RISSafe, monitors operational conflicts, and notifies affected agencies and officers. This is a RISSafe-required function, as all conflicts must have human intervention in order to ensure the safety of agencies and officers who submit operations.

7. *RISSafe Remote Users*

1) When allowed by the RISSafe Watch Center, remote user event registration will be permitted for approved law enforcement users of RISSNET after having successfully completed the training requirements as described under Section 10 of this policy.

2) To maximize the utility of RISSafe, officers should contact their RISSafe Watch Center to initiate the event registration process by telephone, computer, handheld device, fax, or email.

3) RISS member and nonmember agency users may access RISSafe remotely. Each RISS Center will determine whether to permit nonmember remote access in its region. A RISSafe Watch Center may choose to prohibit RISSafe remote user access and instead mandate that the user contact the RISSafe Watch Center to have information submitted to RISSafe.

4) RISSafe restricts the length of events to a maximum of one year in duration. Watch Center personnel may override this restriction, as appropriate.

5) Users will not be able to register an event with a date and time that is prior to the current date and time.

6) Users may register events on a 24/7 basis. RISSafe AOI(s) are monitored on a 24/7 basis, and conflicts shall be responded to as required by this policy.

7) Remote users will make every effort to submit events at least two hours prior to the scheduled event.

8) Remote users shall be able to view only the events that they have registered. RISSafe Watch Center staff members will have the capability of monitoring all events in their AOI.

A Sample Agency Policy is provided in Appendix A to assist agencies that are establishing internal policies on the use of RISSafe.

8. RISSafe Watch Center Operations

1) Agencies wishing to become a RISSafe Watch Center must contact their in-region RISS Center. In order to become a RISSafe Watch Center, an entity must meet the following criteria:

   a) Must be recognized as a law enforcement "center"—such as a RISS Center, a fusion center, or a HIDTA Intelligence Support Center—or is a state law enforcement agency located in the United States or other U.S. territories. Other entities may be considered on a case-by-case basis.
   b) Must be a component of a law enforcement program—such as RISS, HIDTA, fusion centers, etc.—that includes officer safety as part of the organization's mission/objective. RISSafe Watch Center staff may not take independent operational action on investigations.
   c) No private entity may act as a RISSafe Watch Center.
   d) The handling of conflicting operations among overlapping AOIs must be defined by agreement with the appropriate RISSafe Watch Centers monitoring AOIs and with RISS.

2) All entities wishing to act as a RISSafe Watch Center must complete a RISSafe Watch Center Participation Agreement between the entity and RISS (*Appendix B*).

3) All staff members supporting RISSafe must be assigned to a RISSafe Watch Center and are responsible for assisting officers, monitoring activities, responding to conflicts, and notifying affected parties. RISSafe Watch Centers are responsible for specific AOIs.

   a) All RISSafe Watch Center staff members shall receive approved RISSafe training.
   b) Staffing levels shall be appropriate to adequately monitor the RISSafe Watch Center's AOI.
   c) Staff members shall document within RISSafe all contacts made in the process of deconflicting an operation.
   d) RISSafe Watch Centers electing to transfer coverage after regular hours shall arrange and specify such in the established agreement among the appropriate parties.

4) Two or more RISSafe Watch Centers can agree to provide backup support to each other's events. One RISSafe Watch Center will be designated as the primary center for each AOI. Rules established shall be based on the primary RISSafe Watch Center's policies and procedures. A RISS Center established as a RISSafe Watch Center may provide backup support to other RISSafe Watch Centers or other partners, as needed. An agreement between the appropriate parties will be established that defines roles and relationships.

Agencies will send interagency agreements to their in-region RISS Center. RISS Center backup support will be defined in the RISSafe Watch Center Participation Agreement, as appropriate.

5) RISSafe Watch Centers are required to establish local policies and procedures to appropriately verify that requests for submission of events are received only from legitimate law enforcement officers. This verification process is important for overall system security and legitimacy.

6) When a conflict occurs, RISSafe Watch Center staff shall assume responsibility for processing the event and will notify the involved parties of the pending conflict.

7) RISSafe Watch Centers shall provide necessary event and contact information to the involved law enforcement officers so they may make contact and deconflict an event. Disclosure of additional event information will be determined by the involved officers.

8) It is the responsibility of the primary RISSafe Watch Center (for an established AOI) to make the necessary deconfliction notifications to the involved law enforcement officers. The Western States Information Network (WSIN, a RISS Center) will provide nationwide 24/7 backup coverage for all established RISSafe Watch Centers by handling conflicts not addressed by the primary RISSafe Watch Center (or backup support RISSafe Watch Center) within 15 minutes.

9) In the event that WSIN is unable to perform its watch center duties, the Rocky Mountain Information Network (RMIN, a RISS Center) will serve as the nationwide 24/7 backup coverage.

9. *RISSIntel and Other Intelligence Systems*

1) RISSafe is not a criminal intelligence database. Users of RISSafe may enter events with or without the necessity of criminal predicate. All entities entered into RISSafe should also be queried in RISSIntel. Those events that have criminal predicate will be stored in the respective RISS Center instance of RISSIntel or another criminal intelligence system available via the RISSIntel user interface, as appropriate.

2) Any agency with a criminal intelligence database available via the RISSIntel user interface may establish a RISSafe interface to allow the data entered into RISSafe to be transferred and stored in the agency database or in RISSIntel. Only users of agency systems that have established the previously-described RISSafe interface will be presented an option to submit data to their agency

system. Agency intelligence databases must have bidirectional connectivity with the RISSIntel database.

3) RISSafe will identify the appropriate RISSIntel database or agency criminal intelligence systems to store the information. Information will be sent only to one database directly from RISSafe.

4) RISSafe submittal information will be automatically transferred to RISSIntel when the submission is completed (or sent to another criminal intelligence database as previously described). The submittal information will be held in queue for review and processing by the appropriate RISS Center staff or remote user to ensure that the information meets Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations Part 23) requirements before it is saved to RISSIntel.

5) Only users from RISS member agencies will be permitted to store information gathered from RISSafe in the RISSIntel system.

6) After entering an event into RISSafe, if the involved agency determines that initial information was incorrect or invalid, that agency shall ensure that the information is corrected within RISSafe and the appropriate criminal intelligence database. Events can be edited, preexpired, or cancelled only by a RISSafe Watch Center staff member. Remote users should contact their RISSafe Watch Center to request a change.

7) RISSafe reports will not be created that reveal any entity information about subjects, vehicles, phone numbers, organizations, or weapons.

10. Training

RISSafe users shall be required to complete designated training before being permitted to use RISSafe. The RISSafe Remote Officers Users' Guide will serve as the primary document to train users, and the RISSafe Watch Center Users' Guide (*Appendix C and D, respectively*) will act as the primary document to train RISSafe Watch Center staff.

Each RISS Center will be responsible for training staff assigned to RISSafe Watch Centers in its respective region. RISS may provide training to users via train-the-trainer programs, online tutorials, training sessions at one or more of the RISS Center training facilities or at the agency itself, and/or any other appropriate training. Because of the operational nature of RISSafe and for officer safety purposes, the use of demonstration, fictional, or test data is prohibited in the production version of RISSafe. A separate demonstration version of RISSafe (RISSafe Demo) is available for training and testing purposes. Contact your in-region RISS Center for information regarding the demonstration version of RISSafe.

All RISSafe users must acknowledge that they have received training, have read and understand the users' guide, and agree to abide by this policy. The method for users to acknowledge training may be in writing or through an automated process or other mechanism agreed to by RISS and the participating user or agency.

11. RISS Privacy Policy

All RISSafe Watch Centers and RISSafe users must adhere to the RISS Privacy Policy (*Appendix E*). Failure to adhere to the policy may result in the removal of access to RISS services.

12. Evaluation

RISS reserves the right to evaluate RISSafe and its related policies, procedures, and training guidelines, as needed, and to make upgrades, enhancements, and revisions without the consent of users or partnering agencies.

13. Auditing

An audit log will be maintained on RISSafe events and will include canceled events. Audit logs will be kept for the life of the system or until such time that the RNPG determines that records can be purged. RISS maintains the authority to review audit logs at any time, for any reason, to ensure integrity of the system.

Event information within RISSafe shall be retained for statistical purposes in RISSafe for 18 months from the last active date of an event. RISS will, as appropriate and needed, report statistical information on the operations and performance of RISSafe.

14. Liability

Individual RISSafe Watch Centers are responsible for operations, including reviewing events and properly informing appropriate parties on a timely basis when conflicts arise. RISS is not liable for the operations of non-RISS–operated RISSafe Watch Centers, whether they use RISSafe or another similar system. RISS is not responsible for the information entered or provided by the participating law enforcement officers—it is the responsibility of the officer/agency to ensure that the information entered or provided is accurate, timely, and complete.

Participants may not hold RISS liable in any claim, demand, action, suit, or proceeding, including but not limited to, any suit, in law or in equity, for damages by reason of or arising out of any RISSafe event or for any loss, cost, expense, or damages resulting from or arising out of using or relying upon information in RISSafe. To the maximum extent permitted by law, RISS shall not be responsible or liable for any damages whatsoever arising out of or related to the use of or inability to use RISSafe, even if RISS has been advised of the possibility of such damages. This does not constitute a waiver of any defense or immunity lawfully available to RISS.