City of Brisbane
Agenda Report

TO: **HONORABLE MAYOR AND CITY COUNCIL**
Via CLAYTON HOLSTINE, City Manager

FROM: **THOMAS R. HITCHCOCK, Chief of Police**

DATE: **City Council Meeting of September 21, 2009**

SUBJECT: **MEMORANDUM OF UNDERSTANDING WITH THE WEST BAY INFORMATION SHARING SYSTEM**

RECOMMENDATION: Authorize the City Manager and Chief of Police to execute a Memorandum of Understanding (MOU) between the City of Brisbane and law enforcement agencies in San Mateo and San Francisco Counties for records data sharing within the West Bay Information Sharing System.

BACKGROUND: For the past several years, the law enforcement agencies within San Mateo County have been sharing their Computer Aided Dispatch and Records Management System data as part of our regional crime fighting efforts.

This MOU will formalize the records management system data sharing agreements through the West Bay Information Sharing System comprised of law enforcement agencies in San Mateo and San Francisco County. The data node will be installed and hosted by the San Mateo County Sheriff's Office with Federal Homeland Security grant funds that were approved by the Board of Supervisors on July 7, 2009. The grant covers all costs for the project through FY 2011. After that time, the cost to the Police Department is approximately $3,300.00 annually.

The FY07 Urban Area Security Initiative (UASI) Grant Program and the San Francisco Bay Area Urban Area Security Initiative (UASI) is managing a project to establish records management system connectivity between Bay Area law enforcement and justice agencies throughout the State of California through the COPLINK system. COPLINK organizes and rapidly analyzes vast quantities of structured and seemingly unrelated data, housed in various incompatible databases and record management systems, over a highly secure intranet-based platform. Once the statewide COPLINK system has been established, it is anticipated that the MOU will be amended and the West Bay Information Sharing System node will connect to the statewide COPLINK system.

BUDGET IMPACT: There is no budget impact through FY 2011. Beginning in FY 2012, the annual cost paid by the Police Department operating budget would be approximately $3,300.

Thomas Hitchcock, Chief of Police

Clayton Holstine, City Manager

Memorandum of Understanding
West Bay Information Sharing System (WBISS)
WEST BAY REGION NODE

This Memorandum of Understanding ("MOU") is made and entered into on this _____ day of _____2009 by and between the parties below and all future signers of this agreement, known collectively as "Member Agencies" or individually as a "Member Agency."

The following Member Agencies hereby create the West Bay Information Sharing System (WBISS) WEST BAY REGION NODE (Node): The following agencies are collectively known as the "Original Member Agencies."

- Atherton Police Department
- Belmont Police Department
- Brisbane Police Department
- Broadmoor Police Department
- Burlingame Police Department
- Colma Police Department
- Daly City Police Department
- East Palo Alto Police Department
- Foster City Police Department
- Half Moon Bay Police Department
- Hillsborough Police Department
- Menlo Park Police Department
- Millbrae Police Department
- Pacifica Police Department
- Redwood City Police Department
- San Bruno Police Department
- San Carlos Police Department
- San Francisco Police Department
- San Mateo Police Department
- San Mateo County Sheriff's Office
- San Francisco County Sheriff's Office
- South San Francisco Police

Purpose

Member Agencies shall work cooperatively to establish an integrated system of information technology that maximizes the sharing of data and communication between the Member Agencies while maintaining the confidentiality of privileged or otherwise protected information shared through the system. This regional law enforcement information-sharing system shall be known as the WBISS West Bay Region Node. The Member Agencies shall work cooperatively in a variety of ways to facilitate sharing data in an effort to improve the information sharing efforts of their respective Agency and Node. The purpose of this agreement is to define the working relationships, and lines of authority for Member Agencies in the WBISS West Bay Region Node.

San Mateo County Police Chiefs and Sheriff and San Francisco Police Chief and Sheriff, through a grant from the Office of Homeland Security, have indicated the Cities, Counties, and other Agencies within San Mateo and San Francisco Counties, including

any departments or divisions of such agencies, should enter into an agreement to share data among such agencies. The purpose of this document is to create the West Bay Region Node, to outline the duties and responsibilities of each Member Agency, and to provide for the addition of other eligible entities in the data-sharing program created by this MOU.

THEREFORE, the Member Agencies hereby agree to the following:

1 Definitions:

1.1 *West Bay Information Sharing System*: "WBISS" means the collective group of law and justice agencies, within the San Mateo and San Francisco Counties who are signatory on a regional law enforcement information-sharing agreement.

1.2 *West Bay Region Node:* "Node" means the collective informational infrastructure of the data warehouse operated for the benefit of the Member Agencies, within the central region of WBISS who are bound by the terms of this Agreement.

1.3 *West Bay Region Node Board of Chiefs and Sheriffs* means the Police Chief or Sheriff of each Member Agency, or their designee, each of whom shall have equal voting rights in the decisions of the Node.

1.4 *COPLINK*: means the information sharing and analysis software licensed to the Fiscal Agent on behalf of Member Agencies by KCC under the name COPLINK.

1.5 *Data*: means facts, detailed information, or other material provided by a Member Agency.

1.6 *Data Set* is a specific grouping of data included in systems like records management or jail management systems. For example, typical data sets within a records management system include, but are not limited to, Crime Reports, Field Investigations, Citations, Mug shots, and Arrest Reports.

1.7 *Data Records* refers to a unique record associated with an incident or person. For example, this refers to a single report that includes a variety of data.

1.8 *Fiscal Agent*: means the agency, entity or person approved and directed by the Board of Chiefs and Sheriffs to handle and account for funds collected by the Consortium for the benefit of all Member Agencies.

1.9 *Host:* means the entity providing the facilities used to host the Node as determined by a fair review and decision by the Board of Chiefs and Sheriffs.

1.10 *Knowledge Computing Corporation*: "KCC" means a corporation with its principal place of business at 6601 E. Grant Road, Suite 201, Tucson, Arizona 85615, and the owner and developer of COPLINK.

2 Effective Date and Term of MOU

2.1 Effective Date: The effective date of this MOU is the date the last member agency executes this Agreement.

2.2 Term: This MOU shall remain in effect and shall be reviewed and renewed every three years. It can only be terminated as provided herein.

3 Committee and Working Groups

3.1 The West Bay Region Node Board of Chiefs and Sheriffs: shall be comprised of the Police Chief or Sheriff for each Member Agency, or their designee, with each having an equal voice or vote on the direction, decision, and future planning of Node. The Board of Chiefs and Sheriffs shall meet regularly, not less than annually.

3.1.1 The Police Chiefs and Sheriffs Board Chair shall be elected from among the Board of Chiefs and Sheriffs members for a term of no more than two years. The Chair may select a designee to serve on his/her behalf.

3.1.2 The Board of Police Chiefs and Sheriffs shall set policy for the use of the WBISS West Bay Region Node .

3.2 West Bay Region Node Technology Committee: The Board of Police Chiefs and Sheriffs shall appoint a representative from each Member Agency to serve on the Technology Committee. These Technology Committee Members will serve at the sole discretion of the Board of Police Chiefs and Sheriffs. This Technology Committee will implement the policies as set forth by the Board of Police Chiefs and Sheriffs. This committee will meet at least once per year to address system operations, upgrades, enhancements and any other matters of concern to Member Agencies.

3.3 West Bay Region Node Working Groups: The Board of Police Chiefs and Sheriffs is empowered to create, dissolve, or reconstitute working groups, appoint representatives, and perform other actions as deemed

necessary to fulfill the purposes stated herein, including the creation of implementation or sustainment group or other teams necessary to further law enforcement information sharing efforts.

4 Data Access and Security Requirements

4.1 Data Access: Access to Member Agencies' Data will be provided utilizing a secure network maintained by the Host Nodes. The San Mateo County Sheriff's Office will be responsible for the maintenance and care of the secure network in San Mateo County and the City and County of San Francisco will be responsible for the maintenance and care of their secure network. Query capabilities shall be provided to Member Agencies and authorized users utilizing any secure network configuration that is acceptable to the Host Node. The information residing in the Data Repositories shall generally be available to other Member Agencies. Member Agencies agree to inform the other Member Agencies advance, whenever possible, of scheduled down times of specific data feeds.

4.2 Data Sharing: All Member Agencies agree to share data with other Member Agencies who have a need to know and a right to know based on the written guidelines adopted by each Member Agency, with comprehensive, timely, accurate information about a suspect or offender to include, but not limited to, identity, prior agency contacts, citations, arrests, investigations, criminal history, and current justice status. Each agency will be required to have each employee sign an Employee Statement form agreeing not to misuse the information which is contained in Coplink. Each agency will have the prerogative of not sharing those items of data that it deems sensitive or confidential. Nothing in this MOU shall be construed to mean that any Member Agency must share any type of data. The Board of Chiefs and Sheriffs will develop a Guideline Document that will make a recommendation for the type of data to be shared by each agency. This document will be a guideline only and will not be binding. The data to be shared will be the data that the Member Agency already has in its own database and no agency will be required to collect any data that it does not collect in its normal course of business.

The West Bay Region Node Technology Committee will set the criteria for the minimum number of data sets (i.e. Crime Reports, Citations, Field Investigations, Mugs, Arrests Reports, etc.) that member agencies must provide to be a member agency. In addition, the Technology Committee will adopt guidelines for agencies to withhold or suppress certain documents based on specific criteria. Based on these guidelines, each Member Agency shall determine, in the exercise of its sole

discretion, which data records are shared within the system and shall maintain the databases to share the information that has been agreed upon in advance. Each Agency shall strive to identify and achieve common interests to enhance public safety and due process while maintaining individual privacy rights.

4.3 Security Requirements: Member Agencies agree to maintain and enforce security requirements for the system. Each Member Agency is responsible for its internal agency security of their records and any technical support necessary to insure proper security. Member Agencies agree to confirm that their network meets current DOJ security requirements as set forth in the most current Policies, Practices and Procedures Document provided by the Department of Justice, and that it will continue to meet those standards.

4.3.1 Liability and Indemnification: Each Member Agency takes legal and financial responsibility for the actions of their employees, officers, agents, representatives and volunteers. Member Agencies agree to indemnify, defend and hold harmless other Member Agencies to the fullest extent permitted by law from and against any and all demands, claims, actions, liabilities, losses, damages, and costs, including reasonable attorney's fees arising out of or resulting from that Agency's performance under this MOU, and that each agency shall bear the proportionate cost of any damage attributable to the fault of that agency, its governing body, officers, agents, employees and volunteers. It is the intention of the Member Agencies that, where fault is determined to have been contributory, principles of comparative fault will be followed.

4.3.2 Background and Fingerprint Requirements:
All persons including non-criminal justice and volunteer personnel who have access to the WBISS West Bay Region Node are required to undergo background and fingerprint check. Each Agency will determine, based on their internal policies and the CLETS Policies and Procedures when WBISS access will not be granted to an employee.The final responsibility for maintaining the security and confidentiality of WBISS information rests with the Member Agency Chief or designee.

4.3.3 User Access:

It is required that each employee/volunteer sign an employee statement form agreeing to comply with state and federal law prior to operating or having WBISS access. It is recommended that each employee/volunteer sign an employee statement on a biennial basis.

Additional requirements may be added at an agency's discretion. A sample form is included as Exhibit A to this Agreement.

When a person with access to WBISS is no longer employed or no longer accessing WBISS on behalf of the Member Agency, the Agency is responsible for removing all related passwords and security authorizations from the system.

No person with access to WBISS shall release any information or records located in WBISS except to the extent required by law.

4.3.3 Insurance: Each Member Agency, at its sole cost and expense, shall carry insurance -or self-insure - its activities in connection with this MOU, and obtain, keep in force and maintain, insurance or equivalent programs of self-insurance, for general liability, workers compensation, and business automobile liability adequate to cover its potential liabilities hereunder.

4.4 Connecting with other COPLINK Nodes: The Board of Police Chiefs and Sheriffs will continually work to expand the connectivity of the WBISS West Bay Region Node and will actively pursue opportunities to amend this MOU to include other COPLINK nodes under the guidelines outlined in this agreement.

5 Information Ownership, Release and Accuracy

5.1 Ownership and Release Constraints: Member Agencies shall retain control of and remain the official custodian of all information they contribute to the West Bay Region Node. To the extent permitted by law, requests for information under the California Public Records Act or Freedom of Information Act, will be directed back to the Member Agency that is the owner of the requested data, and will be responded to accordingly.

5.2 Information Utilization: Any Data present in the COPLINK system is the proprietary information of the Member Agency contributing that Data. Each Member Agency has an affirmative obligation to assure that all Data complies with 28 CFR Part 23. 28 CFR Part 23 is attached herein as Exhibit C. Member Agencies and authorized users may use the Data for Law Enforcement use only. The Member Agency responsible for contributing the Data shall have sole discretion regarding release of that information.

5.3 Information Accuracy: Member Agencies and authorized users acknowledge that Data maintained in the West Bay Region Node consists of information that may or may not be accurate. Each Member

Agency agrees to do an internal audit of their own data annually in order to review the data for accuracy. A random sampling of different types of data shall be selected by each agency to review and compare their Records System data with the same data in the Coplink system. Each Member Agency agrees to maintain a copy of their internal audit form for review of the Board of Chiefs and Sheriffs on request. A sample form is attached herein as Exhibit B and can be used to help facilitate this audit.

5.4 Audit Trail: An Audit Trail will be maintained to determine who has accessed the data including the date and time.

5.5 Data Errors: It will be the responsibility of Member Agencies to correct data errors that have been identified at that Member's sole cost within a reasonable time, but no later than ninety-days (90) from the date of notification.

6 Funding, Costs, Personnel and Financial Considerations

6.1 Node Costs: Costs for the creation, maintenance and expansion shall be paid as set forth in this Agreement and as may be amended from time to time.

6.2 Participation: To participate in the West Bay Region Node, agencies agree to share costs based on their number of authorized sworn staff.

6.3 Payment Administration: The County of San Mateo shall administer payments to vendors and invoice Member Agencies for their share of cost in accordance with this Agreement.

6.4 Financial Responsibility: Initially, the hardware and software required at each Node will be included in the initial purchase with Grant funding. If any agency elects to join after the initial start-up of the Node, that new Member Agency is responsible for the cost of acquiring and maintaining the hardware, software, and data communication equipment and services needed by their Agency to connect to the Node. It is understood that as the system ages, there may be certain upgrades or maintenance required on the hardware at each of the Member Agencies. These upgrades or maintenance will be the sole responsibility of the Member Agency. Nothing included in this MOU requires any Agency to fund the activities of any other Member Agency. Future upgrades to the Servers and Core Infrastructure of the System will be shared between Member Agencies as indicated in this Agreement. In the event that hardware or software upgrades are required for proper functioning and updated software, the Member Agency will be notified in writing by the Board of Police

Chiefs and Sheriffs at least ninety (90) days in advance of the funding requirement.

6.5 Grant Funding: Grant funding provided by the California Office of Homeland Security will be used to offset the start-up costs for the Node. The primary use of these funds will focus on infrastructure and paying for data integration fees for the original Member Agencies. The County of San Mateo will manage all aspects of payment and reporting for grant funding.

6.6 Future Grant Funding: Member Agencies that apply individually for grant funding for this system should notify the West Bay Region Node Board of Chiefs and Sheriffs to avoid duplicative efforts and requests for funding. Any grant funding which may result from such applications will be considered to be outside of this MOU. The Member Agencies may choose to apply jointly for grant funding and upon the written agreement of the Member Agencies; such monies shall fall under the jurisdiction of this MOU.

6.7 Member Agency Employees: Employees of a Member Agency working for the benefit of the Node remain the employees of that Member Agency.

7 Financial Oversight and Management

7.1 Node Costs: After the Grant Funding is exhausted in 2011, Member Agencies shall pay a proportional share of software purchases, software maintenance, implementationt, network, hardware and operational costs as approved by the West Bay Region Node as approved by the Board of Chiefs and Sheriffs.

7.2 Annual Budget: Each year, San Mateo County Sheriff's Office shall prepare an annual budget for approval by the Board of Chiefs and Sheriffs that includes the share of cost for each Member Agency.

7.3 Annual Report: At least once per year, San Mateo County Sheriff's shall report to the Board of Police Chiefs and Sheriffs on all funds collected and expended by the West Bay Region Node Consortium in support of the COPLINK project.

7.4 Payment Administration: San Mateo County Sheriff's Office shall administer payments to all vendors and invoice Member Agencies for their share of cost.

7.5 Financial Responsibility: The San Mateo County Sheriff's Office will be responsible for the payment of any initial costs to connect to the WBISS Node data repository, which may include acquiring hardware, software, data communication equipment and/or services prior to 2011 out of the 2007 grant award by the Office of Homeland Security. They will pay for the necessary hardware infrastructure for the West Bay Region Node. After 2011, those costs related to maintenance and upgrades to the system will revert to the Member Agencies. Nothing included in this MOU requires any agency to fund the activities of any other Member agency.

7.6 Payment Schedule

7.6.1 Office of Homeland Security: The 2007 grant award by the Office of Homeland Security will pay for the necessary hardware infrastructure for the West Bay Region Node, 100% of the data integration costs for each Member agency, the enterprise software license fee, and two years of maintenance. The following outlines the initial and ongoing maintenance costs for Member Agencies to participate in the WBISS Node. These maintenance costs are subject to review and additional assessment by the Chiefs.

7.6.2 Annual Maintenance: Agency annual maintenance will not be due until 2011. Maintenance costs will be invoiced by the County of San Mateo. The annual payment is due within 30 days of receipt by member agencies. If payment or payment arrangements have not been agreed to, services will be terminated.

To purchase all necessary hardware and start data integration with grant Funding:

Initial Data Mapping/Integration **$999,825.62**

The following estimated maintenance fees includes the software maintenance fees from KCC and the hardware, location and maintenance fees necessary to support the node infrastructure. These ongoing sustainment costs will be due annually after the KCC warranty period is complete and grant funding is exhausted. Estimated to start in **July 2011**.

Annual Maintenance for Node sustainment **$142,817.82** or an approximate cost of **$33.00** per sworn officer, per year.

8 Amendments

8.1 This MOU may be amended in writing.

8.2 Addition of new Member Agencies: If additional agencies choose to become Member Agencies after the signing of this MOU, this agreement shall be amended in writing to include those agencies as signatories.

9 Termination

9.1 MOU Termination: This MOU may be terminated by mutual agreement of all Member Agencies.

9.2 Member Agency Termination: Any Member Agency may terminate its participation in this MOU with or without cause upon thirty-day (30) prior written notice to the Board of Police Chiefs and Sheriffs, unless such termination is prohibited by a grant condition or unless the Member Agency is a Host Node. If the Member Agency wishes to remove Data from the Node after termination of its participation, that Member Agency will be responsible for any costs associated this removal.

9.3 Host Node Termination: A Member Agency that is also the Host of the Node wishing to withdraw as a host or terminating its participation in this MOU must inform the Board in writing no less than one-hundred eighty-days (180) prior to termination. The Board of Police Chiefs and Sheriffs is responsible for locating a successor Host for the Node and assisting in the transition to the new Host.

9.4 County of San Mateo Termination of Role as Fiscal Agent: The County of San Mateo may terminate its role as the financial agent for the Member Agencies with or without cause by informing the Board of Police Chiefs and Sheriffs in writing no less than one-hundred eighty - days (180) prior to termination. The departing County is responsible in locating a successor fiscal agent and help in the transition period. Termination by the County requires a review of financial statements to assure a smooth transition of the books and accounts to the new fiscal agent. Termination of the County of San Mateo as fiscal agent shall not serve to terminate that agency's Member Agency status.

9.5 Other Termination: The Board of Police Chiefs and Sheriffs may remove a Member Agency as a party to this MOU if a majority of the Police Chiefs and Sheriffs determine that the Member Agency is not participating in the manner agreed to within this MOU or other supporting documents or agreements.

10 Miscellaneous

10.1 This MOU is intended to provide for a strategic plan to promote data sharing and should be amended as necessary to accomplish the goal of fully integrating the Member Agencies, future agencies and potential future data sources.

City of Atherton

_____ _____

Jerry Gruber
City Manager
City of Atherton

Date

_____ _____

Glenn Nielsen
Chief of Police
City of Atherton

Date

AGREED to this ___ day of _____, 2009:

City of Belmont

_____ _____

Barry Webb
City Manager
City of Belmont

Date

_____ _____

Donald Mattei
Chief of Police
City of Belmont

Date

AGREED to this ___ day of _____, 2009:

APPROVED AS TO FORM:
HAROLD S. TOPPEL
CITY ATTORNEY

City of Brisbane

_____ _____

Clayton Holstine
City Manager
City of Brisbane

Date

_____ _____

Thomas Hitchcock
Police Chief
City of Brisbane

Date

AGREED to this ___ day of _____, 2009:

City of Broadmoor

_____ _____

Greg Love
Police Chief
City of Broadmoor

Date

_____ _____

Greg Love
District Manager
City of Broadmoor

Date

AGREED to this ___ day of _____, 2009:

City of Burlingame

_____ _____

James Nantell
City Manager
City of Burlingame

Date

_____ _____

Jack VanEtten
Police Chief
City of Burlingame

Date

AGREED to this ___ day of _____, 2009:

Town of Colma

_____ _____

Laura Allen
City Manager
Town of Colma

Date

_____ _____

Robert Lotti
Police Chief
Town of Colma

Date

AGREED to this ___ day of _____, 2009:

City of Daly City

_____ _____

Patricia Martel
City Manager
City of Daly City

Date

_____ _____

Gary McLane
Police Chief
City of Daly City

Date

AGREED to this ___ day of _____, 2009:

City of Foster City

_____ _____

Craig Courtin
Police Chief
City of Foster City

Date

_____ _____

Jim Hardy
City Manager
Foster City

Date

AGREED to this ___ day of _____, 2009:

City of East Palo Alto

_____ _____

Alvin James
City Manager
City of East Palo Alto

Date

_____ _____

Ron Davis
Police Chief
City of East Palo Alto

Date

AGREED to this ___ day of _____, 2009:

City of Half Moon Bay

_____ _____

Michael Dolder
City Manager
City of Half Moon Bay

Date

_____ _____

Don O'Keefe
Police Chief
City of Half Moon Bay

Date

AGREED to this ___ day of _____, 2009:

Town of Hillsborough

_____ _____

Anthony Constantouros — Date
City Manager
Town of Hillsborough

_____ _____

Matthew O'Connor — Date
Police Chief
Town of Hillsborough

AGREED to this ___ day of _____, 2009:

City of Menlo Park

_____ _____

Glen Rojas — Date
City Manager
City of Menlo Park

_____ _____

Bruce Goitia — Date
Police Chief
City of Menlo Park

AGREED to this ___ day of _____, 2009:

City of Millbrae

_____ _____

Marcia Raines Date
City Manager
City of Millbrae

_____ _____

Lee Violett Date
Police Chief
City of Millbrae

AGREED to this ___ day of _____, 2009:

City of Pacifica

_____ _____

Clay Phillips Date
City Manager
City of Pacifica

_____ _____

James Saunders Date
Police Chief
City of Pacifica

AGREED to this ___ day of _____, 2009:

City of Redwood City

_____ _____

Peter Ingram
City Manager
City of Redwood City

Date

_____ _____

Louis A. Cobarruviaz
Police Chief
City of Redwood City

Date

AGREED to this ___ day of _____, 2009:

City of San Bruno

_____ _____

Connie Jackson
City Manager
City of San Bruno

Date

_____ _____

Neil Telford
Police Chief
City of San Bruno

Date

AGREED to this ___ day of _____, 2009:

City of San Carlos

_____ _____

Mark Weiss Date
City Manager
City of San Carlos

_____ _____

Greg Rothaus Date
Police Chief
City of San Carlos

AGREED to this ___ day of _____, 2009:

City of South San Francisco

_____ _____

Barry Nagel Date
City Manager
City of South San Francisco

_____ _____

Michael Massoni Date
Police Chief
City of South San Francisco

AGREED to this ___ day of _____, 2009:

City and County of San Francisco

_____ _____

Heather Fong
Police Chief
City of San Francisco

Date

_____ _____

Gavin Newsom
Mayor
City of San Francisco

Date

_____ _____

Michael Hennessey
Sheriff
County of San Francisco

Date

AGREED to this ___ day of _____, 2009:

City of San Mateo

_____ _____

Susan Loftus Date
City Manager
City of San Mateo

_____ _____

Susan Manheimer Date
Police Chief
City of San Mateo

AGREED to this ___ day of _____, 2009:

County of San Mateo

_____ _____

David Boesch Date
County Manager
County of San Mateo

_____ _____

Greg Munks Date
Sheriff
County of San Mateo

AGREED to this ___ day of _____, 2009:

Exhibit A

EMPLOYEE/VOLUNTEER STATEMENT FORM

As an employee/volunteer of _____, you may have access to confidential records stored in the WBISS West Bay Information Sharing System. All access is based on the "need to know" and the "right to know." Misuse of such information may adversely affect an individual's civil rights, and violates the law and/or WBISS policy.

Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11141-11143 and 13302-13304 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records .

"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information not authorized by law to receive the record or information is guilty of a misdemeanor."

Any employee/volunteer who is responsible for WBISS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL
WBISS ACCESSIBLE INFORMATION.

_____ _____

Signature Print Name

Date _____

Exhibit B

COPLINK

ANNUAL DATA AUDIT FOR DATA ACCURACY

Date	Time	Data Type	Data	Verified in Coplink?

Exhibit C

28 CFR Part 23
CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES
Executive Order 12291
1998 Policy Clarification
1993 Revision and Commentary

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. 23.1 Purpose. 23.2 Background. 23.3 Applicability. 23.20 Operating principles. 23.30 Funding guidelines. 23.40 Monitoring and auditing of grants for the funding of intelligence systems. Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c). § 23.1 Purpose. The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals. § 23.2 Background. It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required. § 23.3 Applicability. (a) These policy standards are

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

means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy. § 23.20 Operating principles. (a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. (b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. (c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and

audit procedures established by the project. (d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. (e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity. (f) (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles. (2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property. (g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained

participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented: (1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system; (2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project; (3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization; (4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster; (5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and (6) A project may authorize and utilize remote (off-premises)

system data bases to the extent that they comply with these security requirements. (h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years. (i) If funds awarded under the Act are used to support the operation of an intelligence system, then: (1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and (2) A project shall undertake no major modifications to system design without prior grantor agency approval. (j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award. (k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance. (l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation. (m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system. (n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

- 4 -

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any

applicable state or federal law. § 23.30 Funding guidelines. The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria: (a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity. (b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and: (1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and (2) Involve a significant degree of permanent criminal organization; or (3) Are not limited to one jurisdiction. (c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20. (d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency: (1) assume official responsibility and accountability for actions taken in the name of the joint entity, and (2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system. (e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation. § 23.40 Monitoring and auditing of grants for the funding of intelligence systems. (a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20. (c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the

continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson Acting Assistant Attorney General Office of Justice Programs (FR Doc. 93-22614 Filed 9-15-93; 8:45 am) Criminal Intelligence Sharing Systems; Policy Clarification [Federal Register: December 30, 1998 (Volume 63, Number 250)] [Page 71752-71753] From the Federal Register Online via GPO Access [wais.access.gpo.gov] DEPARTMENT OF JUSTICE 28 CFR Part 23 [OJP(BJA)-1177B] RIN 1121-ZB40

- 6 -
1993 Revision and Commentary

28 CFR Part 23 Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies

---

AGENCY: Office of Justice Programs, Justice.

ACTION: Final Rule SUMMARY: The regulation governing criminal intelligence systems operating through support under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines. EFFECTIVE DATE: September 16, 1993 FOR FURTHER INFORMATION CONTACT: Paul Kendall, Esquire, General Counsel, Office of Justice Programs, 633 Indiana Ave., NW., Suite 1245-E, Washington, DC 20531, Telephone (202) 307-6235. SUPPLEMENTARY INFORMATION: The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the Federal Register on February 27, 1992, (57 FR 6691). The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows: Confidentiality of Information

Sec. 812....

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.

(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

This statutory provision and its implementing regulation apply to intelligence systems funded under title I of the Act, whether the system is operated by a single law enforcement agency, is an interjurisdictional intelligence system, is

funded with discretionary grant funds, or is funded by a State with formula grant funds awarded under the Act's Drug Control and System Improvement Grant Program pursuant to part E, subpart 1 of the Act, 42 U.S.C. 3751-3759. The need for change to 28 CFR part 23 grew out of the program experience of the Office of Justice Programs (OJP) and its component agency, the Bureau of Justice Assistance (BJA), with the regulation and the changing and expanding law enforcement agency need to respond to criminal mobility, the National drug program, the increased complexity of criminal networks and conspiracies, and the limited funding available to State and local law enforcement agencies. In addition, law enforcement's capability to perform intelligence data base and analytical functions has been enhanced by technological advancements and sophisticated analytical techniques.

- 7 -

28 CFR part 23 governs the basic requirements of the intelligence system process. The process includes:

1. Information submission or collection 2. Secure storage 3. Inquiry and search capability 4. Controlled dissemination 5. Purge and review process

Information systems that receive, store and disseminate information on individuals or organizations based on reasonable suspicion of their involvement in criminal activity are criminal intelligence systems under the regulation. The definition includes both systems that store detailed intelligence or investigative information on the suspected criminal activities of subjects and those which store only information designed to identify individuals or organizations that are the subject of an inquiry or analysis (a so-called "pointer system"). It does not include criminal history record information or identification (fingerprint) systems. There are nine significant areas of change to the regulation:

(1) Nomenclature changes (authority citations, organizational names) are included to bring the regulation up to date.

(2) Definitions of terms (28 CFR 23.3(b)) are modified or added as appropriate. The term "intelligence system" is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation; the terms "interjurisdictional intelligence system", "criminal intelligence information", "participating agency", "intelligence project", and "validation of information" are key terms that are defined in the regulation for the first time.

(3) The operating principles for intelligence systems (28 CFR 23.20) are modified to define the term "reasonable suspicion" or "criminal predicate". The finding of reasonable suspicion is a threshold requirement for entering intelligence information on an individual or organization into an intelligence data base (28 CFR 23.20(c)). This determination, as well as determinations that information was legally obtained (28 CFR 23.20(d)) and that a recipient of the information has a need to know and a right to know the information in the performance of a

law enforcement function (28 CFR 23.20(e)), are established as the responsibility of the project for an interjurisdictional intelligence system. However, the regulation permits these responsibilities to be delegated to a properly trained participating agency which is subject to project inspection and audit (28 CFR 23.20(c),(d),(g)).

(4) Security requirements are established to protect the integrity of the intelligence data base and the information stored in the data base (28 CFR 23.20(g)(1)(i)-(vi)).

(5) The regulation provides that information retained in the system must be reviewed and validated for continuing compliance with system submission criteria within a 5-year retention period. Any information not validated within that period must be purged from the system (28 CFR 23.20(h)).

(6) Another change continues the general prohibition of direct remote terminal access to intelligence information in a funded intelligence system but provides an exception for systems which obtain express OJP approval based on a determination that the system has adequate policies and procedures in place to insure that access to system intelligence information is limited to authorized system users (28 CFR 23.20(i)(1)). OJP will carefully review all requests for exception to assure that a need exists and that system integrity will be provided and maintained (28 CFR 23.20(i)(1)).

(7) The regulation requires participating agencies to maintain back-up files for information submitted to an interjurisdictional intelligence system and provide for inspection and audit by project staff (28 CFR 23.20(h)).

(8) The final rule also includes a provision allowing the Attorney General or the Attorney General's designee to authorize a departure from the specific requirements of this part, in those cases where it is clearly shown that such waiver would promote the purposes and effectiveness of a criminal intelligence system while at the same time ensuring compliance with all applicable laws and protection for the privacy and constitutional

rights of individuals. The Department recognizes that other provisions of federal law may be applicable to (or may be adopted in the future with respect to) certain submitters or users of information in criminal intelligence systems. Moreover, as technological developments unfold over time in this area, experience may show that particular aspects of the requirements in this part may no longer be needed to serve their intended purpose or may even prevent desirable technological advances. Accordingly, this provision grants the flexibility to make such beneficial adaptations in particular cases or classes without the necessity to undertake a new rulemaking process. This waiver authority could only be exercised by the Attorney General or designee, in writing, upon a clear and convincing showing (28 CFR 23.20 (o)).

(9) The funding guidelines (28 CFR 23.30) are revised to permit funded intelligence systems to collect information either on organized criminal activity that represents a significant and recognized threat to the population or on

criminal activity that is multi-jurisdictional in nature. Rulemaking History On February 27, 1992, the Department of Justice, Office of Justice Programs, published a notice of proposed rulemaking in the Federal Register (57 FR 6691). The Office of Justice Programs received a total of eleven comments on the proposed regulation, seven from State agencies, two from Regional Information Sharing Systems (RISS) program fund recipients, one from a Federal agency, and one from the RISS Project Directors Association. Comments will be discussed in the order in which they address the substance of the proposed regulation. Discussion of Comments Title - Part 23 Comment: One commentor suggested reinserting the word "Operating" in the title of the regulation to read "Criminal Intelligence Systems Operating Policies" to reflect that the regulation applies only to policies governing system operations. Response: Agreed. The title has been changed. APPLICABILITY - SECTION 23.3(a) Comment: A question was raised by one respondent as to whether the applicability of the regulation under Section 23.3(a) to systems "operating through support" under the Crime Control Act included agencies receiving any assistance funds and who operated an intelligence system or only those who received assistance funds for the specific purpose of funding the operation of an intelligence system. Response: The regulation applies to grantees and subgrantees who receive and use Crime Control Act funds to fund the operation of an intelligence system. Comment: Another commentor asked whether the purchase of software, office equipment, or the payment of staff salaries for a criminal intelligence system would constitute "operating through support" under the Crime Control Act. Response: Any direct Crime Control Act fund support that contributes to the operation of a criminal intelligence system would subject the system to the operation of the policy standards during the period of fund support. Comment: A third commentor inquired whether an agency's purchase of a telephone pen register or computer equipment to store and analyze pen register information would subject the agency or its information systems to the regulation. Response: No, neither a pen register nor equipment to analyze telephone toll information fall under the definition of a criminal intelligence system even though they may assist an agency to produce investigative or other information for an intelligence system. APPLICABILITY - SECTION 23.3(b) Comment: Several commentors questioned whether information systems that are designed to collect information on criminal suspects for purposes of inquiry and analysis, and which provide for dissemination of such information, qualify as "criminal intelligence systems." One pointed out that the information qualifying for system submission could not be "unconfirmed" or "soft" intelligence. Rather, it would generally have to be

: One respondent asked whether the definition of criminal intelligence system covered criminal history record information (CHRI) systems, fugitive files, or other want or warrant based information systems. investigative file-based information to meet the "reasonable suspicion" test. Response: The character of an information system as a criminal intelligence system does not depend upon the source or categorization of the underlying information as "raw" or "soft" intelligence, preliminary investigation information, or investigative information,

findings or determinations. It depends upon the purpose for which the information system exists and the type of information it contains. If the purpose of the system is to collect and share information with other law enforcement agencies on individuals reasonably suspected of involvement in criminal activity, and the information is identifying or descriptive information about the individual and the suspected criminal activity, then the system is a criminal intelligence system for purposes of the regulation. Only those criminal intelligence systems that receive, store and provide for the interagency exchange and analysis of criminal intelligence information in a manner consistent with this regulation are eligible for funding support with Crime Control Act funds. Comment

Response: No. A CHRI system contains information collected on arrests, detention, indictments, informations or other charges, dispositions, sentencing, correctional supervision, and release. It encompasses systems designed to collect, process, preserve, or disseminate such information. CHRI is factual, historical and objective information which provides a criminal justice system "profile" of an individual's past and present involvement in the criminal justice system. A fugitive file is designed to provide factual information to assist in the arrest of individuals for whom there is an outstanding want or warrant. Criminal intelligence information, by contrast, is both factual and conjectural (reasonable suspicion), current and subjective. It is intended for law enforcement use only, to provide law enforcement officers and agencies with useful information on criminal suspects and to foster interagency coordination and cooperation. A criminal intelligence system can have criminal history record information in it as an identifier but a CHRI system would not contain the suspected criminal activity information contained in a criminal intelligence system. This distinction provides the basis for the limitations on criminal intelligence systems set forth in the operating policies. Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system. Comment: Another commentor asked whether a law enforcement agency's criminal intelligence information unit, located at headquarters, which authorizes no outside access to information in its intelligence system, would be subject to the regulation. Response: No. The sharing of investigative or general file information on criminal subjects within an agency is a practice that takes place on a daily basis and is necessary for the efficient and effective operation of a law enforcement agency. Consequently, whether such a system is described as a case management or intelligence system, the regulation is not intended to apply to the exchange or sharing of such information when it takes place within a single law enforcement agency or organizational entity. For these purposes, an operational multi-jurisdictional task force would be considered a single organizational entity provided that it is established by and operates under a written memorandum of understanding or interagency agreement. The definition of "Criminal Intelligence System" has been modified to clarify this point. However,

if a single agency or entity system provides access to system information to outside agencies on an inquiry or request basis, as a matter of either policy or practice, the system would qualify as a criminal intelligence system and be subject to the regulation. Comment: A commentor questioned whether the proposed exclusion of "analytical information and work products" from the definition of "Intelligence System" was intended to exclude all dissemination of analytical results from coverage under the regulation. Response: No. The exceptions in the proposed definition of "Intelligence System" of modus operandi files, historical telephone toll files and analytical information and work products are potentially confusing. The exceptions reflect types of data that may or may not qualify as "Criminal Intelligence Information" depending on particular facts and circumstances. Consequently, these exceptions have been deleted from the definition

- 10 -

: One commentor requested clarification of the role of the "Project" in the operation of an intelligence system, i.e. is the project required to have physical control (possession) of the information in an intelligence system or will authority over the system (operational control) suffice? : Operational control over an intelligence system's intelligence information is sufficient. The regulation seeks to establish a single locus of authority and responsibility for system information. Once that principle is established, the regulation permits, for example, the establishment of remote (off premises) data bases that meet applicable security requirements. of "Intelligence System" in the final rule. For example, analytical information and work products that are derived from unevaluated or bulk data (i.e. information that has not been tested to determine that it meets intelligence system submission criteria) are not intelligence information if they are returned to the submitting agency. This information and its products cannot be retained, stored, or made available for dissemination in an intelligence system unless and until the information has been evaluated and determined to meet system submission criteria. The proposed definition of "Analytical Information and Work Products" in Section 23.3(b) has also been deleted. To address the above issues, the definition of "Intelligence System" has been modified to define a "Criminal Intelligence System or Intelligence System" to mean "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information." Comment: Several commentors raised questions regarding the concept of "evaluated data" in the definition of "Criminal Intelligence Information", requesting guidance on what criteria to use in evaluating data. Another questioned whether there needed to be an active investigation as the basis for information to fall within the definition and whether information on an individual who or organization which is not the primary subject or target of an investigation or other data source, e.g. a criminal associate or co-conspirator, can qualify as "Criminal Intelligence Information." Response: The definition of "Criminal Intelligence Information" has been revised to reflect that data is evaluated for two purposes related to criminal intelligence system submissions: (1) to determine that it is relevant in identifying a criminal suspect

and the criminal activity involved; and (2) to determine that the data meets criminal intelligence system submission criteria, including reasonable suspicion of involvement in criminal activity. As rewritten, there is no requirement that an "active investigation" is necessary. Further, the revised language makes it clear that individuals or organizations who are not primary subjects or targets can be identified in the criminal intelligence information, provided that they independently meet system submission criteria. CommentResponseOPERATING PRINCIPLES - SECTION 23.20(c) Comment: One respondent took the position that "Reasonable Suspicion", as defined in Section 23.20 (c), is not necessary to the protection of individual privacy and Constitutional rights, suggesting instead that information in a funded intelligence system need only be "necessary and relevant to an agency's lawful purposes." Response: While it is agreed that the standard suggested is appropriate for investigative or other information files maintained for use by or within an agency, the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of "hits" in an information system is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural. Comment: The prior commentor also criticized the proposed definition of reasonable suspicion for its specific reference to an "investigative file" as the source of intelligence system information, the potential inconsistency between the concepts of "infer" and "conclude" as standards for determining whether reasonable suspicion is justified by the information available, and the use of "reasonable possibility" rather than "articulable" or "sufficient" facts as the operative standard to conclude that reasonable suspicion exists. Response: The reference to an "investigative file" as the information source has been broadened to encompass any information source. The information available must provide a basis for the submitter to "believe" there is a reasonable possibility of the subject's involvement in the criminal activity or enterprise.

The concept of a "basis to believe" requires reasoning and logic coupled with sound judgment based on experience in law enforcement rather than a mere hunch, whim, or guess. The belief that is formed, that there is a "reasonable possibility" of criminal involvement, has been retained because the proposed standard is appropriately less restrictive than that which is required to establish probable cause.

OPERATING PRINCIPLES - SECTION 23.20(d) Comment: Section 23.20(d) prohibits the inclusion in an intelligence system of information obtained in violation of Federal, State, or local law or ordinance. Would a project be potentially liable for accepting, maintaining and disseminating such information even if it did not know that the information was illegally obtained? Response: In addition to protecting the rights of individuals and organizations that may be subjects in a criminal intelligence system, this prohibition serves to protect a

project from liability for disseminating illegally obtained information. A clear project policy that prohibits the submission of illegally obtained information, coupled with an examination of supporting information to determine that the information was obtained legally or the delegation of such authority to a properly trained participating agency, and the establishment and performance of routine inspection and audit of participating agency records, should be sufficient to shield a project from potential liability based on negligence in the performance of its intelligence information screening function. OPERATING PRINCIPLES - SECTION 23.20(h) Comment: One commentor requested clarification of the "periodic review" requirement in Section 23.20(h) and what constitutes an "explanation of decision to retain" information.

Response: The periodic review requirement is designed to insure that system information is accurate and as up-to-date as reasonably possible. When a review has occurred, the record is appropriately updated and notated. The explanation of decision to retain can be a variety of reasons including "active investigation", "preliminary review in progress", "subject believed still active in jurisdiction", and the like. When information that has been reviewed or updated and a determination made that it continues to meet system submission criteria, the information has been "validated" and begins a new retention period. The regulation limits the retention period to a maximum of five years without a review and validation of the information. OPERATING PRINCIPLES - SECTION 23.20(i) Comment: One commentor requested a definition of "remote terminal" and asked how OJP would determine whether "adequate policies and procedures" are in place to insure the continued integrity of a criminal intelligence system.
Response: A "remote terminal" is hardware that enables a participating agency to input into or access information from a project's criminal intelligence data base without the intervention of project staff. While the security requirements set forth in Section 23.20(g)(1)-(5) should minimize the threat to system integrity from unauthorized access to and the use of system information, special measures are called for when direct remote terminal access is authorized. The Office of Justice Programs will expect any request for approval of remote terminal access to include information on the following system protection measures: 1. Procedures for identification of authorized remote terminals and security of terminals; 2. Authorized access officer (remote terminal operator) identification and verification procedures; 3. Provisions for the levels of dissemination of information as directed by the submitting agency; 4. Provisions for the rejection of submissions unless critical data fields are completed; 5. Technological safeguards on system access, use, dissemination, and review and purge; 6. Physical security of the system;

7. Training and certification of system-participating agency personnel; 8. Provisions for the audit of system-participating agencies, to include: file data supporting submissions to the system; security of access terminals; and policy and procedure compliance; and 9. Documentation for audit trails of the entire system operation. Moreover, a waiver provision has been added to ensure

flexibility in adapting quickly to technological and legal changes which may impact any of the requirements contained in this regulation. See Section 23.20 (o). Comment: Related to the above discussion, another commentor asked whether restrictions on direct remote terminal access would prohibit remote access to an "index" of information in the system. Response: Yes. The ability to obtain all information directly from a criminal intelligence system through the use of hardware based outside the system constitutes direct remote terminal access contrary to the provisions of Section 23.20(i)(1), except as specifically approved by OJP. Thus, a hit/no hit response, if gleaned from an index, would bring a remote terminal within the scope of the requirement for OJP approval of direct remote terminal access. Comment: One commentor pointed out that the requirement for prior OJP approval of "modifications to system design" was overly broad and could be read to require that even minor changes be submitted for approval. The commentor proposed a substitute which would limit the requirement to those modifications "that alter the system's identified goals in a way contrary to the requirements of (this regulation)."

Response: While it is agreed that the language is broad, the proposed limitation is too restrictive. The intent was that "modifications to system design" refer to "major" changes to the system, such as the nature of the information collected, the place or method of information storage, the authorized uses of information in the system, and provisions for access to system information by authorized participating agencies. This clarification has been incorporated in the regulation. In order to decentralize responsibility for approval of system design modifications, the proposed regulation has been revised to provide for approval of such modifications by the grantor agency rather than OJP. A similar change has been made to Section 23.20(j). OPERATING PRINCIPLES - SECTION 23.20(n) Comment: Several commentors expressed concern with the verification procedures set forth in Section 23.20(n). One suggested that file information cannot "verify" the correctness of submissions but instead serves to "document" or "substantiate" its correctness. Another proposed deleting the requirements that (1) files maintained by participating agencies to support system submissions be subject to the operating principles, and (2) participating agencies are authorized to maintain such files separately from other agency files. The first requirement conflicts with the normal investigative procedures of a law enforcement agency in that all information in agency source files cannot meet the operating principles, particularly the reasonable suspicion and relevancy requirements. The important principle is that the information which is gleaned from an agency's source files and submitted to the system meet the operating principles. The second requirement has no practical value. At most, it results in the creation of duplicative files or in submission information being segregated from source files. Response: OJP agrees with both comments. The word "documents" has been substituted for "verifies" and the provisions subjecting participating agency source files to the operating principles and authorizing maintenance of separate files have been deleted. Projects should use their audit and inspection access to agency source files to document the correctness of participating agency submissions on a sample basis. FUNDING GUIDELINES -

SECTION 23.30(b) Comment: One commentor asked: Who defines the areas of criminal activity that "represent a significant and recognized threat to the population?" Response: The determination of areas of criminal activity focus and priority are matters for projects, project policy boards and member agencies to determine, provided that the additional regulatory requirements set forth in Section 23.30(b) are met. MONITORING AND AUDITING OF GRANTS - SECTION 23.40(a)

- 13 -

Comment: One commentor asked: "Who is responsible for developing the specialized monitoring and audit of awards for intelligence systems to insure compliance with the operating principles"?

Response: The grantor agency (the agency awarding a sub-grant to support an intelligence system) shall establish and approve a plan for specialized monitoring and audit of sub-awards prior to award. For the BJA Formula Grant Program, the State agency receiving the award from BJA is the grantor agency. Technical assistance and support in establishing a monitoring and audit plan is available through BJA. INFORMATION ON JUVENILES Comment: Can intelligence information pertaining to a juvenile who otherwise meets criminal intelligence system submission criteria be entered into an intelligence data base? Response: There is no limitation or restriction on entering intelligence information on juvenile subjects set forth in Federal law or regulation. However, State law may restrict or prohibit the maintenance or dissemination of such information by its law enforcement agencies. Therefore, State laws should be carefully reviewed to determine their impact on this practice and appropriate project policies adopted.

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

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) 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. . (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) 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 Validation of Information § 23.20 Operating principlesReasonable 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

- 16 -

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

- 17 -

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

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation. § 23.40 Monitoring and auditing of grants for the funding of intelligence systems. (a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds. (b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20. (c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies. Laurie Robinson Acting Assistant Attorney General Office of Justice Programs (FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

- 18 -

1998 Policy Clarification

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is

appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of "criminal intelligence system" is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by 28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

Comments

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is "information 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 . . . meets criminal intelligence system submission criteria." Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual if "there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 CFR 23.20(b) extends that limitation to [page 71753] collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 CFR Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing "Comment" or "Modus Operandi" fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the

- 19 -

identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional "Northwest Market." An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of "Northwest Market" would not be permitted, because there was no reasonable suspicion that the "Northwest Market" was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the "Northwest Market" was clearly noted to be non-criminal in nature. For example, the data field in which "Northwest Market" was entered could be marked "Non-Criminal Identifying Information," or the words "Northwest Market" could be followed by a parenthetical comment such as "This organization has been entered into the system for identification purposes only - it is not suspected of any criminal activity or involvement." A criminal intelligence system record or file could not be created for "Northwest Market" solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on "Northwest Market." Further, the fact that other individuals frequent "Northwest Market" would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

The Definition of a "Criminal Intelligence System"

The definition of a "criminal intelligence system" is given in 28 CFR 23.3(b)(1) as the "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information . . . ." Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

The comments to the 1993 revision of 28 CFR Part 23 noted that "the term 'intelligence system' is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation . . . ." 58 FR 48448-48449 (Sept. 16, 1993.) The comments further noted that materials that "may assist an agency to produce investigative or other information for an intelligence system . . ." do not necessarily fall under the regulation. Id.

The above rationale for the exclusion of non-intelligence information sources from the definition of "criminal intelligence system," suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

- 20 -

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

Additional guidelines will be issued to provide details of the above clarifications as needed.

Dated: December 22, 1998.

Nancy Gist Director, Bureau of Justice Assistance [FR Doc. 98-34547 Filed 12-29-98; 8:45 am] BILLING CODE 4410-18-P

- 21 -