MEMORANDUM OF UNDERSTANDING FOR: The Commonwealth Fusion Center ("CFC") and the Commonwealth's Information Technology Division ("ITD").

PURPOSE: This Memorandum of Understanding (MOU) sets forth policies, procedures and guidelines for ITD in support of Law Enforcement Agencies (LEAs) and establishes parameters within which ITD may provide support to the CFC.

Whereas, the CFC is empowered to enter into this Memorandum of Understanding; and

Whereas, ITD is empowered to enter into this Memorandum of Understanding; and

Now, THEREFORE, it is agreed:

AUTHORITIES
This MOU is entered into under the authority of the laws of the Commonwealth of Massachusetts.

TERMS OF AGREEMENT
CFC DUTIES
The Massachusetts State Police will establish workspace within the CFC and will provide those computer and telephonic connections necessary for ITD's personnel to perform assigned duties in furtherance of the CFC's goals/mission. Direct access to computer applications and the Internet will be provided to each outside agency member assigned at the CFC. Access to any other online searchable databases will be provided on a contingent basis through CFC staff members. Intelligence products produced by the CFC may be made available to each outside agency member upon request, in accordance with CFC policy.

ITD DUTIES
ITD employees assigned to the CFC shall be directed by the decisions of the Commanding Officer of the CFC for all matters occurring in the normal course of business of the CFC.
In all matters concerning ITD employees' salary, benefits, administration of personnel records and other administrative needs, the member is subject to the supervision of their own agency.

While assigned to the CFC, the assigned ITD employee will:

- Assist CFC personnel with requests for information and all other matters relating to criminal investigations by providing access to ITD databases and resources, subject to ITD policies regarding data and system access.
- Assist CFC staff with the collection, collation, and vetting of incoming information for processing and dissemination of intelligence products.
- Share all relevant ITD intelligence with the CFC in a timely manner.

- Ensure appropriate information is entered into the CFC Intelligence System.
- Provide adequate coverage and assign/delegate an alternative member during times of absence to enable timely access and effective utilization of ITD resources.
- Record daily activities through the CFC blotter to ensure accurate data is included in the Performance Measures Report.

DURATION AND TERMINATION

This MOU shall remain in effect until such time as a signatory agency withdraws from the agreement. ITD or the CFC may withdraw from this agreement upon a 30-day notice in writing to the CFC.

AUTHORIZED REPRESENTATIVES

The CFC's authorized representative for the purposes of administration of this agreement is Major Robert G. Smith or his successor. ITD's authorized representative for the purposes of administration of this agreement is Stephen Nardone, ITD's Chief Technology Officer, or his/her successor.

FINANCIAL RESPONSIBILITIES

Participating employees will carry out designated functions at their own agency's expense, including salaries, benefits and local transportation.

ASSIGNMENT

Neither the CFC nor ITD shall assign or transfer any rights or obligations under this agreement without the prior written consent of the other party.

AMENDMENTS

Amendments to this MOU shall be proposed by the CFC Commanding Officer, and approved by all signatories to this MOU.

LIABILITY

The CFC and ITD agree that each party will be responsible for its own acts, or the acts of its Representative(s) and the results thereof to the extent authorized by law and shall not be responsible for the acts of any others and the results thereof. The CFC's and ITD's liability shall be governed by the provisions of Massachusetts law and other applicable law.

SECURITY

The Commanding Officer of the CFC, currently Major Robert G. Smith, or his designee shall be responsible for establishing appropriate security measures to ensure the integrity of the operations of the CFC.

The Commanding Officer shall report on security measures to the Colonel/Superintendent of State Police on a periodic basis. Any breach of security shall immediately be reported to the Colonel/Superintendent of State Police.

The Commanding Officer of the CFC shall be responsible for ensuring that appropriate background checks have been made on each employee assigned to the CFC and each employee who is authorized to receive information from the Center. The Commanding Officer of the CFC shall have the discretionary authority to deny the assignment of an individual to the CFC and/or deny access to any information or the facility itself for security reasons.

The CFC shall utilize the "Third Agency Rule," meaning dissemination of another agency's materials beyond the CFC requires advanced permission from the originating agency. In addition, no agency shall disseminate materials pertaining to criminal justice information produced by the CFC without first obtaining the permission of the Commanding Officer of the CFC, or his/her designee. These rules shall apply to all individuals assigned to the CFC, regardless of their agency.

THE INFORMATION SECURITY COMPLIANCE AGREEMENT

The CFC has established the Information Security Compliance Agreement to ensure that the rights of innocent citizens are not abridged by the operations of the CFC, and ITD agrees to abide by it. The Information Security Compliance Agreement is attached hereto as Appendix A. Contingent upon receipt of federal funding to support CFC operations, CFC personnel and all ITD personnel assigned to the CFC shall abide by the rules of intelligence sharing as defined by Section 28 of the Code of Federal Regulations, Part 23, attached hereto as Appendix B.

DISPUTE RESOLUTION

Any disputes that may arise between the participating agencies concerning the operations of the CFC shall be referred to the Commanding Officer for resolution. If the Commanding Officer cannot resolve the dispute, it will be referred to the Agency Heads of the parties involved for resolution.

OTHER PROVISIONS

The parties agree to abide by the terms of the CFC-ITD Job Description attached hereto as Appendix C. It is hereby attached and incorporated by reference.

IN FURTHERANCE of their respective goals, objectives, and missions, the parties jointly agree to abide by the provisions of this MOU.

IN WITNESS WHEREOF, the parties hereto have caused this MOU to be duly executed.

APPROVED:

1. **AGENCY**

By: 

Peter Quinn

Title: _____CIO, Information Technology Division___

Date: 8/11/05

2. **MASSACHUSETTS STATE POLICE**
COMMONWEALTH FUSION CENTER

By: _____
Colonel Thomas G. Robbins

Title: Superintendent, Massachusetts State Police

Date: 8/11/05

Distribution:
Executive Office of Public Safety & Homeland Security
Colonel/Superintendent's Office, MSP

APPENDIX B

§ 22.28 Use of data identifiable to a private person for judicial, legislative or administrative purposes.

(a) Research or statistical information identifiable to a private person shall be immune from legal process and shall only be admitted as evidence or used for any purpose in any action, suit, or other judicial, legislative or administrative proceeding with the written consent of the individual to whom the data pertains.

(b) Where consent is obtained, such consent shall:

(1) Be obtained at the time that information is sought for use in judicial, legislative or administrative proceedings;

(2) Set out specific purposes in connection with which information will be used;

(3) Limit, where appropriate, the scope of the information subject to such consent.

[41 FR 54846, Dec. 15, 1976, as amended at 45 FR 62038, Sept. 18, 1980]

§ 22.29 Sanctions.

Where BJA, OJJDP, BJS, NIJ, or OJP believes that a violation of section 812(a) of the Act or section 1407(d) of the Victims of Crime Act, these regulations, or any grant or contract conditions entered into thereunder has occurred, it may initiate administrative actions leading to termination of a grant or contract, commence appropriate personnel and/or other procedures in cases involving Federal employees, and/or initiate appropriate legal actions leading to imposition of a civil penalty not to exceed $10,000 for a violation occurring before September 29, 1999, and not to exceed $11,000 for a violation occurring on or after September 29, 1999 against any person responsible for such violations.

[Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]

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).

SOURCE: 58 FR 48452, Sept. 16, 1993, unless otherwise noted.

§ 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:

APPENDIX B

(l) *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.

APPENDIX B

(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.

(ii) [Reserved]

APPENDIX B

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99–508, 18 U.S.C. 2510–2520, 2701–2709 and 3121–3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

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

§ 23.30 Funding guidelines.

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

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d)(1) 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 policy-making authority who has been expressly delegated such control and supervision by the head of the agency:

APPENDIX B

(i) Assume official responsibility and accountability for actions taken in the name of the joint entity, and

(ii) 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.

(2) 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.

PART 24—IMPLEMENTATION OF THE EQUAL ACCESS TO JUSTICE ACT IN DEPARTMENT OF JUSTICE ADMINISTRATIVE PROCEEDINGS

Subpart A—General Provisions

Sec.

Subpart B—Information Required From Applicants

Subpart C—Procedures for Considering Applications

AUTHORITY: 5 U.S.C. 504(c)(1).

SOURCE: Order No. 975-82, 47 FR 15776, Apr. 13, 1982, unless otherwise noted.

Subpart A—General Provisions

§ 24.101 Purpose of these rules.

These rules are adopted by the Department of Justice pursuant to section 504 of title 5, U.S. Code, as amended by section 203(a)(1) of the Equal Access to Justice Act, Public Law No. 96-481. Under the Act, an eligible party may receive an award for attorney fees and other expenses when it prevails over the Department in an adversary adjudication under 5 U.S.C. 554 before the Department, unless the Department's position as a party to the proceeding was substantially justified or special circumstances make an award unjust. The purpose of these rules is to establish procedures for the submission and consideration of applications for awards against the Department.

§ 24.102 Definitions.

As used in this part:

(a) *The Act* means section 504 of title 5, U.S. Code, as amended by section 203(a)(1) of the Equal Access to Justice Act, Public Law No. 96-481.

(b) *Adversary adjudication* means an adjudication under 5 U.S.C. 554 in which the position of the United States