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 submit-
ting agencies and control officials.
Each project must establish written
definitions for the need to know and
right to know standards for dissemina-
tion 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 informa-
tion being requested either through in-
quiry or by delegation of this responsi-
bility to a properly trained partici-
pating agency which is subject to rou-
tine inspection and audit procedures
established by the project. Each intel-
ligence project shall assure that the
following security requirements are
implemented:
(1) Where appropriate, projects must
adopt effective and technologically ad-
vanced computer software and hard-
ware 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 informa-
tion in the system in a manner such
that it cannot be modified, destroyed,
accessed, or purged without authoriza-
ton;
(4) The project must institute proce-
dures to protect criminal intelligence
information from unauthorized access,
threat, 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 author-
ized to have direct access to the sys-
tem; and
(6) A project may authorize and uti-
lize remote (off-premises) system data
bases to the extent that they comply
with these security requirements.
(b) All projects shall adopt proce-
dures to assure that all information
which is retained by a project has rel-
evancy and importance. Such proce-
dures shall provide for the periodic re-
view of information and the destruc-
tion of any information which is mis-
leading, obsolete or otherwise unreli-
able and shall require that any recipi-
ent 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 re-
viewer, date of review and explanation
of decision to retain. Information re-
tained in the system must be reviewed
and validated for continuing compli-
ance with system submission criteria
before the expiration of its retention
period, which in no event shall be
longer than five (5) years.
(1) If funds awarded under the Act are
used to support the operation of an in-
telligence system, then:
(1) No project shall make direct re-
 mote terminal access to intelligence
information available to system par-
ticipants, except as specifically ap-
proved by the Office of Justice Pro-
grams (OJP) based on a determination
that the system has adequate policies
and procedures in place to insure that
it is accessible only to authorized sys-
tems users; and
(2) A project shall undertake no
major modifications to system design
without prior grantor agency approval.
(ii) [Reserved]
(j) A project shall notify the grantor
agency prior to initiation of formal in-
formation exchange procedures with
any Federal, State, regional, or other
information systems not indicated in
the grant documents as initially ap-
poved 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 elec-
tronic, mechanical, or other device for
surveillance purposes that is in viola-
tion 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 applica-
table State statute related to wire-
tapping and surveillance.
(l) A project shall make assurances
that there will be no harassment or in-
terference with any lawful political ac-
tivities as part of the intelligence op-
eration.
§ 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 policy-making authority who has been expressly delegated such control and supervision by the head of the agency:

(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