

any administrative costs paid by the issuer, and the certification under paragraph (d)(6)(iii)(D) of this section.

(3) For each bid that is submitted, the name of the person and entity submitting the bid, the time and date of the bid, and the bid results.

(4) The bid solicitation form and, if the terms of the purchase agreement or the guaranteed investment contract deviated from the bid solicitation form or a submitted bid is modified, a brief statement explaining the deviation and stating the purpose for the deviation. For example, if the issuer purchases a portfolio of investments for a yield restricted defeasance escrow and, in order to satisfy the yield restriction requirements of section 148, an investment in the winning bid is replaced with an investment with a lower yield, the issuer must retain a record of the substitution and how the price of the substitute investment was determined. If the issuer replaces an investment in the winning bid portfolio with another investment, the purchase price of the new investment is not covered by the safe harbor unless the investment is bid under a bidding procedure meeting the requirements of this paragraph (d)(6)(iii).

(5) For purchases of investments other than guaranteed investment contracts, the cost of the most efficient portfolio of State and Local Government Series Securities, determined at the time that the bids were required to be submitted pursuant to the terms of the bid specifications.

(e) \* \* \*

(2) \* \* \*

(iv) *Special rule for investments purchased for a yield restricted defeasance escrow.* For investments purchased for a yield restricted defeasance escrow, a fee paid to a bidding agent is a qualified administrative cost only if the following requirements are satisfied:

(A) The fee is comparable to a fee that would be charged for a reasonably comparable investment if acquired with a source of funds other than gross proceeds of tax-exempt bonds, and it is reasonable. The fee is deemed to be comparable to a fee that would be charged for a comparable investment acquired with a source of funds other than gross proceeds of tax-exempt bonds, and to be reasonable if the fee does not exceed the lesser of \$10,000 or .1% of the initial principal amount of investments deposited in the yield restricted defeasance escrow.

(B) For transactions in which a guaranteed investment contract and other investments are purchased for a yield restricted defeasance escrow in a

single investment (e.g., an issuer bids United States Treasury obligations and an escrow float contract collectively), a broker's fee described in paragraph (e)(2)(iv)(A) of this section will apply to the initial principal amount of the investment deposited in the yield restricted defeasance escrow, and a broker's fee described in paragraph (e)(2)(iii) of this section will apply only to the guaranteed investment contract portion of the investment.

\* \* \* \* \*

**PART 602—OMB CONTROL NUMBERS UNDER THE PAPERWORK REDUCTION ACT**

**Par. 3.** The authority citation for part 602 continues to read as follows:

**Authority:** 26 U.S.C. 7805.

**Par. 4.** In § 602.101, paragraph (c) is amended by revising the entry for 1.148-5 in the table to read as follows:

**§ 602.101 OMB Control numbers.**

\* \* \* \* \*

(c) \* \* \*

CFR part or section where identified and described	Current OMB control No.
* * * * *	* * * * *
1.148-5 .....	1545-1098, 1545-1490
* * * * *	* * * * *

Approved: December 17, 1998.

**Robert E. Wenzel,**  
*Deputy Commissioner of Internal Revenue.*

**Donald C. Lubick,**  
*Assistant Secretary of the Treasury.*  
[FR Doc. 98-34209 Filed 12-29-98; 8:45 am]  
BILLING CODE 4830-01-U

**DEPARTMENT OF JUSTICE**

**28 CFR Part 23**

[OJP(BJA)-1177B]

RIN 1121-ZB40

**Criminal Intelligence Sharing Systems; 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 N.W., Washington, D.C. 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 \* \* \* [m]eets 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

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 C.F.R. § 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 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 "[t]he 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. 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

---

## DEPARTMENT OF TRANSPORTATION

### Coast Guard

#### 33 CFR Part 100

[CGD 95-054]

RIN 2115-AF17

#### Regattas and Marine Parades

**AGENCY:** Coast Guard, DOT.

**ACTION:** Interim rule; delay of effective date.

---