17th St. & Constitution Avenue N.W.
Washington, D.C. 20006
United States of America

Organization of American States

P. 202.458.3000
www.oas.org

INTER-AMERICAN DRUG ABUSE
CONTROL COMMISSION

CICAD

Secretariat for Multidimensional Security

XXXIII MEETING OF THE GROUP OF EXPERTS FOR THE CONTROL
OF MONEY LAUNDERING
September 17 - 18, 2012
Buenos Aires, Argentina

OEA/Ser.L/XIV. 4.33
CICAD/LAVEX/doc.4/14
18 September 2011
Original: Spanish

# RECOMMENDED PRINCIPLES FOR THE COORDINATION AND INTEGRATION OF FIU/OIC WORKING GROUP

# RECOMMENDED PRINCIPLES ON THE USE AND PROTECTION OF FIU INFORMATION

**Recommended Principles for the Coordination and Integration of FIU/OIC Working Group**

**Organization of American States, Inter-American Drug Abuse Control Commission (OAS/CICAD)**

**On the Use and Protection of FIU Information**

## Introduction

A financial intelligence unit (FIU) is an agency within a jurisdiction that collects, analyzes and disseminates information for anti-money laundering and counter financing of terrorism (AML/CFT) purposes. FIUs have unique authority to exchange information with their foreign counterparts in furtherance of law enforcement investigations.

The FIU information exchange is premised on trust and reciprocity. Therefore, many of the Organization of American States (OAS) member states are concerned with confidentiality breaches of FIU information in their region.

In several cases information derived from a foreign FIU to further develop a criminal investigation and eventual prosecution has been disclosed to unauthorized third parties, including the criminal defendant or even to the general public by a range of government officials. In many instances, the disclosure might have been avoided if there were a more consistent understanding among all parties involved of the need to treat FIU information differently from other information that might have been developed in the course of the investigation.

At the XXXII Meeting of the Group of Experts for the Control of Money Laundering, held in Washington D.C. in May 2011, a number of FIUs in the region identified some of the challenges that they face in keeping FIU information confidential when it is shared with law enforcement, prosecutors and the judicial authorities (third parties). At that meeting it was noted that information shared between FIUs is intended to identify intelligence leads, not to be used as evidence in court or divulged to any unauthorized third parties.

FIU reports and communications are highly sensitive in nature because they often contain private and personal identifiable information of citizens and legal persons who have not been found guilty of a crime. Leaks of FIU information may have a devastating effect on the reputation of those whose personal information has been divulged inappropriately, especially if they are not charged with a crime or if they are not found guilty after prosecution. Leaks can also compromise law enforcement investigations, alert targets of an inquiry and erode the trust of reporting entities in the AML/CFT regime.

If left unchecked, the leaks of FIU information will seriously undermine cooperative efforts to combat financial crime in the region. A direct consequence of this type of breach is the

breakdown of trust and willingness to cooperate between FIUs in the exchange of sensitive information. In fact, there have been instances where information exchange has been suspended between FIUs due to unauthorized disclosures of FIU information.

Many of the OAS member states have noted similar challenges that their FIUs face in working with law enforcement, prosecutors and judicial authorities to protect sensitive FIU information and a general misunderstanding by some prosecutors and law enforcement of the proper use of FIU information. It has also been noted that FIUs do not feel responsible for leaks that occur outside of their FIU, once information is forwarded to third parties.

Given the above, the OAS member states should consider fundamental that their FIUs follow rigorously the Egmont Group "Principles for Information Exchange among Financial Intelligence Units for Money Laundering and Terrorism Financing Cases" adopted at The Hague, on June 2001, which are included below. These principles refer to the process by which FIUs share information that they collect and analyze. These principles do not govern the sharing of information between law enforcement and prosecutors via formal channels, such as mutual legal assistance treaties and letters rogatory.

Furthermore, it is considered the OAS member states would benefit from adopting the recommended principles for the use and protection of FIU information shared with FIUs and authorized third parties, which are also included below.

These principles are meant to outline generally-shared concepts, while allowing countries to maintain necessary flexibility. A follow-up piece to this document will discuss best practices involving the use and protection of FIU information.

# Proposed Principles for the Use and Protection of FIU Information

## I. FIU-to-FIU Information Exchange[1]

### *A. Introduction*

1. The Egmont Group works to foster the development of Financial Intelligence Units ("FIUs")[2] and information exchange.

2. The Egmont Group agreed in its Statement of Purpose, adopted in Madrid on 24 June 1997, to pursue among its priorities the stimulation of information exchange and to overcome the obstacles preventing cross-border information sharing.

3. Information-sharing arrangements should have the aim of fostering the widest possible co-operation between FIUs.

4. The following principles for information exchange among FIUs are meant to outline generally-shared concepts, while allowing countries the necessary flexibility.

### *B. General Framework*

5. International co-operation between FIUs should be encouraged and based upon a foundation of mutual trust.

6. FIUs should take steps to seek information that may be used by other identified domestic law enforcement or financial supervisory agencies engaged in enforcement and related regulatory activities.

7. FIUs should work to encourage that their jurisdiction's national legal-standard and privacy laws are not conceived so as to inhibit the exchange of information, in accordance with these principles, between or among FIUs.

8. Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.

---

[1] Source: The Egmont Group of Financial Intelligence Units (FIUs), Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases, The Hague, 13 June 2001.

[2] For more information on the Egmont Group and FIUs, see the Egmont Group's web site: www.egmontgroup.org.

### *C. Conditions for the Exchange of Information*

9. FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party. Such exchange, either upon request or spontaneously, should produce any available information that may be relevant to an analysis or investigation of financial transactions and other relevant information and the persons or companies involved.

10. An FIU requesting information should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the receiving FIU to determine whether the request complies with its domestic law.

### *D. Permitted Uses of Information*

11. Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.

12. The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information.

### *E. Confidentiality–Protection of Privacy*

13. All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with national provisions on privacy and data protection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU.

## Principles for FIU Information Sharing Between Financial Intelligence Units and Third Parties

### A. Responsibilities of FIUs vis-à-vis law enforcement, prosecutors and judiciary authorities ("Third Parties")

Recognizing that as the primary point of contact and gateway for financial intelligence information, FIUs are accountable to their foreign counterparts for the protection of information that they receive from those counterparts through sharing mechanisms:

1. The FIU that wishes to share foreign FIU information with Third Parties must obtain prior authorization from the foreign FIU and must notify in writing the Third Parties that the foreign FIU's information is for intelligence purposes only.

2. The FIU information cannot be used as evidence within an administrative, investigative, prosecutorial or judicial process without the prior consent of the requested FIU. Even if permission is granted to use FIU information as evidence, there may be additional legal requirements such as those in Mutual Legal Assistance Treaties (MLATS) and the use of letters rogatory, for the information to be used as evidence in legal proceedings.

3. In order to protect the information that an FIU receives from foreign FIUs, the FIU should take steps to raise awareness on the part of Third Parties on the proper use and protection of FIU information.

4. FIUs that receive information from foreign FIUs and intend to share that information with Third Parties must collaborate with Third Parties to ensure that the Third Parties take necessary measures to maintain the confidentiality of the foreign FIU's information.

5. In cases of an unauthorized disclosure of a foreign FIU's information, the FIU in possession of a foreign FIU's information must immediately notify that foreign FIU if it discovers that a misuse or unauthorized disclosure of FIU information has occurred. The FIU in possession of a foreign FIU's information must take immediate action to remedy the situation, limit further disclosure, work with the foreign FIU to resolve the matter, and provide certainty that future similar situations will not occur.

**B. Responsibilities of Third Parties vis-à-vis FIUs**

1. Third Parties requesting foreign FIU information from their national FIU should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the foreign FIU to determine whether the request complies with its domestic law;

2. Third Parties must follow appropriate FIU procedures in handling FIU information when receiving FIU information that their jurisdiction's FIU has obtained from a foreign FIU;

3. Authorized Third Parties must protect FIU information from dissemination to and access by unauthorized parties;

4. Third Parties that have received FIU information from a foreign FIU may only use the FIU information for intelligence purposes (i.e., as lead information) unless they obtain the prior consent of the foreign FIU.

5. Third Parties cannot use foreign FIU information as evidence within an administrative, investigative, prosecutorial or judicial process absent prior consent of the requested FIU. Even if permission is granted to use FIU information as evidence, there may be additional legal requirements such as those in Mutual Legal Assistance Treaties (MLATS) and the use of letters rogatory, for the information to be used as evidence in legal proceedings.

6. Third Parties may use FIU information only for the specific purpose for which the information was sought or provided;

7. Third Parties cannot share a foreign FIU's information with other third parties (e.g., with other competent authorities) without the prior consent of the requested FIU;

8. Third Parties cannot use FIU information to circumvent formal information sharing mechanisms such as mutual legal assistance treaties or letters rogatory to produce evidence; and

9. Third Parties in possession of foreign FIU information must immediately inform their country's FIU if it discovers that a misuse or unauthorized disclosure of FIU information has occurred. The FIU in possession of a foreign FIU's information must take immediate action to remedy the situation, limit further disclosure, work with the foreign FIU to resolve the matter, and provide certainty that future similar situations will not occur.