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

XXXIV MEETING OF THE GROUP OF EXPERTS FOR THE CONTROL OF MONEY LAUNDERING
MAY 30-31, 2012
Washington DC

OEA/Ser.L/XIV. 4.34
CICAD/LAVEX/doc.2/12
11 May 2012
Original: English

RECOMMENDED BEST PRACTICES FOR THE COORDINATION AND INTEGRATION OF FIU/OIC WORKING GROUP

As of April 26, 2012

Recommended Best Practices 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

In several cases information derived from a Financial Intelligence Unit (FIU) in one jurisdiction to further develop a criminal investigation by law enforcement agencies and eventual prosecution by prosecutorial authorities in another jurisdiction, has been disclosed to unauthorized third parties. 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. To increase awareness, the Integration of FIU/OIC Working Group of the Organization of American States, Inter-American Drug Abuse Control Commission created the Principles on the Use and Protection of FIU Information.

Consistent with the Principles on the Use and Protection of FIU Information, FIUs must design and implement internal systems, procedures and controls to guarantee the confidentiality of information they receive from foreign counterparts and share with authorized stakeholders. This includes their own reports and other documentation that contain information derived from the original source, which may be a foreign FIU or other entity in a foreign jurisdiction. Because it is as important to ensure the appropriate use and protection of FIU information by third parties as it is by FIUs, systems, procedures and controls must take into account best practices from the time the information is received from a foreign FIU to the time that it is disseminated to third parties and beyond, or the same is destroyed. Such systems, procedures and controls must ensure that the information that belongs to a foreign jurisdiction, as well as any reference to the name of the foreign institution that shared the information, are duly protected from unauthorized disclosures. Such systems, procedures and controls shall include, but not be limited to the following:

FIU Personnel Handling FIU Information

- The FIU must carefully select the staff responsible for receiving and handling information from foreign jurisdictions. New staff should undergo a background investigation to ensure that only those with high integrity and honesty are hired to handle FIU sensitive information.

- FIU employees, contractor personnel and consultants with access to foreign FIU information must be aware and comply with safeguarding requirements for FIU's sensitive information, especially information belonging to a foreign jurisdiction.
- Personnel with access to sensitive FIU information must be aware that divulging FIU's sensitive information without proper authority could have serious consequences, including administrative or disciplinary action (i.e. termination).
- FIUs should provide adequate and continuous training to employees to recognize and safeguard sensitive information supporting their mission and operations.

Reception of FIU Information

- When an FIU receives sensitive or equivalent information from another FIU, the information must be handled in accordance with the guidance provided by the sending FIU. Where no guidance is provided it shall be handled in accordance with receiving FIU's policy.
- FIUs should accept information requests and responses from overseas electronically and that information should be encrypted for transmission purposes. Likewise, FIUs should respond to a requestor, using the same secure system that the originator of the request used to transmit the information.
- The sender of a request for information determines if the information should be sent via an encrypted e-mail or other means. If the sender of a request determines e-mail provides sufficient protection and sends the information electronically, the recipient may communicate in the same way when responding.

Categorizing Foreign FIU Information as Sensitive

- As a general rule, receiving FIUs should handle all information provided by another FIU as "sensitive", and may only use it for the specific purpose for which the information was sought or provided.
- When sent outside of FIUs, sensitive information documents must include a statement alerting the recipient in a transmittal letter or directly on the document containing FIU's sensitive information.

> *For example:* This document belongs to the FIU's sensitive information (cite FIU name). It may not be released without the express permission of (cite creating FIU). Refer requests and inquiries for the document to: (insert name and address of originating FIU).

General Handling Procedure

- FIUs may not transfer information shared by a foreign FIU to a third party without the prior consent of the FIU that disclosed the information. Furthermore, the FIU and authorized third parties (if any) may not make use of the foreign FIU information with an administrative, investigative, prosecutorial or judicial purpose without the prior written consent of the FIU that disclosed the information.
- All FIUs should use the greatest caution when dealing with information provided by another FIU, in order to prevent any unauthorized use resulting in a breach of confidentiality.
- The information from another FIU will be treated and protected with the same secrecy and confidentiality as any information belonging to the receiving FIU.
- FIUs should implement a special register to monitor and control the foreign FIUs' financial intelligence reports and information. The special register should contain information on the requestor, the date that the request was received, entered, assigned to an analyst and responded, and organized in a way that allows for the development of statistical reports, including the evaluation of the efficiency of cooperation.

Protection from Unauthorized Disclosures by Third Parties

  - It is recommended that FIUs maintain two bundles: the Principal Docket and the Docket of Information Exchange, plus a back up of the latter in a lock box. This practice may be a good solution for those intelligence units which, by law, must make financial information available to the judiciary of the country.
  - FIUs should note in the Principal file (the one which originates the request) the requirement made to a foreign counterpart.
  - At the onset of a relationship between the FIU and third parties with access to the FIU information, it is recommended that FIUs draft memoranda of understanding establishing the conditions of the information sharing relationship.

- Internal e-mail systems provide sufficient safeguards to allow for the transmission of FIU's sensitive information when the FIU operates within a local area network.
- FIU's sensitive information may be reproduced on regular office copiers to the extent needed to carry out official business.
- A cover sheet should be used to prevent unauthorized or inadvertent disclosure when FIU's sensitive information is removed from an authorized storage location and persons without a need-to-know are present or casual observation would reveal FIU's sensitive information.
- Information received from other foreign FIUs may not be transferred to any other body and/or legal persons or individuals without the express consent of the unit that provided the information.

- When forwarding foreign FIU's information, a cover sheet shall be placed inside the envelope and on top of the transmittal letter, memorandum or document.
- When there is a need to hand carry hard copies of FIU sensitive information across floors and/or departments within the FIU, the documentation should be in a single opaque envelope/container and sealed to prevent inadvertent opening and to reveal evidence of possible tampering. The envelope/container shall bear the complete name of the sender and intended recipient.

Storage

- FIU's sensitive information shall be stored, at a minimum, in a file cabinet, desk drawer, overhead storage bin, credenza, or similar locked compartment.
- FIU's sensitive information may be stored in a room or area with physical access control measures such as a key-locked room, or restricted access work area controlled by a cipher lock or card reader.

Dissemination and Access

- Access to foreign FIU's sensitive information must be on a need-to-know basis as determined by the holder of the information. However, where there is uncertainty as to a person's need-to-know, the holder of the information shall request dissemination instructions from his or her next level supervisor or manager.
- Holders of a foreign FIU's information must comply with any additional access and/or dissemination restrictions that may be cited on the document.
- FIUs requesting information from foreign FIUs must disclose the intended recipient of the information. Authorization for disclosure to additional parties must be obtained prior to further dissemination.
- The foreign FIU's name must be concealed as the source, as well as other identifiers such as document control numbers before the requesting FIU shares that information with third parties.
- Law enforcement agencies with access to Suspicious Transaction Reports (STRs) and information derived from the local FIU or in connection to information received from a foreign FIU, should use it as lead information that when investigated, may produce evidence of criminal activity.
- FIUs should sign memoranda of understanding (MOU) with third parties that will have access to the FIU's information at the onset of an information sharing relationship.
- The FIU should require the users, requestor and recipients of its information to maintain a copy or annotation of the warning about sensitivity with all FIU-related documents as it is

shared within the agency, with joint law enforcement investigating agencies, or with prosecutors.

- As the information is shared, greater vulnerability exists in that the recipients may have lesser understanding of the sensitive nature of the information. Thus, the FIUs should keep a log of the FIU information and/or foreign FIU information that they provide to other agencies.

Protective Orders

- In cases where judicial authorities insist on presenting foreign FIU and/or STRs as evidence in court proceedings, FIUs should (if their national laws allow it) consider working with the Office of the Prosecutor to request protective orders against the disclosure of such information. The FIU's legal department should reach out to its counterpart within the jurisdiction's judicial branch to determine the scope and due process of such legal instruments.

Incident Reporting

- Employees or contractor personnel who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of a foreign FIU's sensitive information shall report it immediately, but not later than the next business day, to their FIU's security or other competent officials, or head of the FIU if a security or other competent department does not exist.
- The head of the FIU or official acting on his/her behalf shall immediately notify the head of the foreign FIU whose sensitive information was disclosed to an unauthorized party.
- The head of the FIU or official acting on his/her behalf having detected an unauthorized disclosure of a foreign FIU's sensitive information shall order a full investigation to determine the details and prepare a report for dissemination to the foreign FIU that provided the information, including the following:

    a. Whether or not an incident actually occurred. If there was no loss, compromise, or unauthorized disclosure, the person(s) in charge of the investigation shall so state;
    b. The events leading to the unauthorized disclosure;
    c. What information was disclosed, whether the information was law enforcement sensitive;
    d. How the information was disclosed;
    e. Who was the information disclosed to;
    f. Who within the government has gained access to the information;
    g. The responsible person(s);

h. The cause of the incident;
i. Actions taken to minimize damage or neutralize the potential for further compromise;

- The FIU must maintain the fact that an unauthorized disclosure has occurred as confidential as possible from the time it learns about the breach until the end of its investigation.

Third Parties' Accountability

- If a breach of information belonging to a foreign FIU is detected but a responsible person(s) within the FIU is not identified, the FIU should contact outside holders of the information such as law enforcement and the prosecutor's office with whom the information may have been shared. Upon contacting the agencies the FIU should explain the roles and responsibilities of authorized holders of foreign FIU sensitive information, according to the Principles on the Use and Protection of FIU Information.
- The FIU shall assist the third party or request to identify any documentation that may have been received from the local FIU containing information in connection to a foreign FIU.
- If after reviewing the third party's response the FIU detects an unauthorized disclosure, it must request that the third party conduct a full investigation to determine the details and prepare a report for dissemination to the foreign FIU that includes the following information:

    a. Confirmation of dissemination of the FIU report containing foreign FIU information;
    b. Whether the information was shared with natural or legal persons, orally or in writing, domestically or internationally to counterparts or others through letters rogatory and/or mutual legal assistance treaties;
    c. What information was disclosed;
    d. The responsible person(s);
    e. Actions taken to minimize damage or neutralize the potential for further compromise.

- Following the request by the FIU of the third party to conduct an investigation into the events that led to the unauthorized disclosure, the FIU should:

    a. Negotiate, if appropriate the signing of Memoranda of Understanding (MOUs) with those stakeholders (users of FIU information) about the appropriate use and protection of FIU information;

b. If necessary, the FIU should share guidelines for use and protection of reports with its local stakeholders such as law enforcement, judicial authorities, and prosecutors using its information.

- STRs and information derived from the local FIU or in connection to information received from a foreign FIU, should be used as lead information that when investigated, may produce evidence of criminal activity.
- FIUs and third parties should never disclose the fact that an STR exists, or that an STR has been filed locally or in a foreign jurisdiction to (1) any person that is the subject of the STR; (2) private entities seeking information pursuant to ongoing litigation; or (3) any non-competent third-party agencies (i.e., entities other than from the central, state or local government agencies supporting examinations of financial institutions, investigations, prosecutions or conduction of intelligence/counterintelligence activities to protect against money laundering or international terrorism);
- FIUs and third parties should never attach or reference STRs or information belonging to a foreign FIU in affidavits for search/seizure warrants, subpoenas, indictments, charging documents, motions, or responses to motions, or press releases.
- It is recommended that when storing these documents, relevant authorities separate STRs from official case files and take additional precautions when uploading case files with numerous STRs to a CD or flash drive.
- In some jurisdictions, Reports of Investigation (ROIs) prepared by law enforcement personnel are subject to discovery by defendants in criminal cases, thus ROIs should describe the transactions and should not make reference to STRs or contain any information which would reveal that an STR has been filed.
- Third parties should always use the underlying transaction records provided by the FIU as evidence in the prosecution's case-not the STR or the information provided by a foreign FIU-which merely constitute unsubstantiated allegations/suspicion.