FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF INSPECTOR GENERAL
Policies and Procedures Manual

PART	**I**	**Operations Policies and Procedures**
SECTION	**OIG-110**	**General Management Policies and Procedures**
CHAPTER	**110.4**	**Confidential Sources**

1. Purpose. To provide policy and guidance on Office of Inspector General (OIG) Confidential Sources (CS) and related confidential documents.

2. Definitions

a. Confidential Source. Any person who provides information to the OIG on a confidential basis.

b. Complainant. Any person who makes a complaint to the OIG concerning the possible existence of fraud, waste, or mismanagement affecting the Federal Deposit Insurance Corporation's (FDIC) programs and operations. There are three types of complainants.

(1) Employee Complainant. Any FDIC employee who makes a complaint to the OIG.

(2) Public Complainant. Any person who is not an FDIC employee who makes a complaint to the OIG.

(3) Anonymous Complainant. A person who makes a complaint without disclosing his/her identity.

c. Witness. Any individual, including an FDIC employee, who provides information or evidence; who testifies or is asked to be present at a transaction to testify to its having taken place; or who has personal knowledge of something as evidence or proof.

d. Contact. Generally, the contact is the OIG staff member responsible for having initially developed the CS. Contacts may introduce an alternate OIG contact to the CS.

3. Legislative Provisions

a. The Inspector General Act of 1978, as amended states the following:

(1) The Inspector General may receive and investigate complaints or information from an employee of the establishment concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety.
(5. U.S.C., App. 3 §7(a))

(2) The Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation. (5. U.S.C., App. 3 §7(b))

(3) Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to an Inspector General, unless the complaint was made or the information disclosed with the knowledge that it was false or with willful disregard for its truth or falsity. (5. U.S.C., App. 3 §7(b))

b. The Whistleblower Protection Act of 1989 (5 U.S.C. §1213) established the Office of Special Counsel (OSC) as a separate agency. The OSC provides a means for complainants to report allegations of violations of laws, rules and regulations, gross mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to public health and safety without fear of retaliation and without disclosure of identity. Retaliation for such disclosure to the Inspector General is specifically prohibited.

4. Policy

a. The responsible Assistant Inspector may designate an individual as a CS when conditions warrant such a designation. This authority to designate a CS may be delegated to senior OIG managers in the field and headquarters, as appropriate. However, complainants and witnesses differ in their rights to confidentiality. The following is OIG policy regarding confidentiality for the three types of complainants and for witnesses:

(1) Employee Complainants. Pursuant to the Inspector General Act of 1978, as amended, an FDIC employee complainant may be designated as a Confidential Source (CS).

However, regardless of whether an employee complainant is specifically designated as a CS, after receipt of a complaint or information from the employee, the OIG will not disclose the identity of the employee without the employee's consent, unless the Inspector General or designee determines such disclosure is unavoidable during the course of the investigation. The Assistant Inspector General who designated an individual as a confidential source may determine whether such disclosure is unavoidable, and authorize disclosure. Any decision on whether the employee will also be treated as a confidential source will be determined on a case by case basis under paragraph 5. Confidentiality may be waived by subsequent actions by the complainant. A case-by-case determination as to such waivers must be made in consultation with OIG Counsel.

(2) Public Complainants. Confidentiality should not be provided to public complainants unless they specifically request it.

(3) Anonymous Complainants. Anonymous complainants cannot be treated as confidential sources because their identity has not been disclosed to the OIG. However, in receiving their complaints, the OIG Contact should ask anonymous complainants to identify themselves in order to facilitate an OIG inquiry. If identification is given, the complainant should be treated as appropriate under subparagraph 1, 2, or 4.

(4) Witnesses. Confidentiality should not normally be provided to witnesses regarding information they submit in response to questions concerning an official inquiry. If the witness initiates a complaint regarding a different matter, confidentiality may be granted to the witness for that information only if the witness is an FDIC employee or requests confidentiality.

b. A contact may ask a CS to provide information already in his/her possession, or to provide information that comes to his/her attention concerning subjects of authorized OIG activity.

c. It should never be expressed or implied to a CS that his/her identity will never be released. The OIG staff shall not disclose the identity of any CS without the individual's consent, unless the Inspector General or designee determines such disclosure is unavoidable during the course of an audit or investigation.

d. Efforts should be made to independently verify the information provided by a CS without jeopardizing the confidentiality of the CS.

e. The contact should be alert to any situation that might be construed as an abuse of the CS's status and, if necessary, inform the CS of the following:

(1) The assistance of the CS is strictly voluntary;

(2) The CS's relationship with the OIG will not protect him/her from arrest or prosecution for any violation of Federal, state, or local law; and/or

(3) The CS supply of information to the OIG does not make him/her an OIG employee, nor should such a status ever be claimed by the CS.

f. In carrying out any request, the CS will not be encouraged or requested to participate in any acts of violence, initiate or instigate a plan to commit criminal acts, or use unlawful techniques to obtain information. If the contact has reason to believe that the CS may engage in such activities, the contact should immediately report that concern to his or her supervisor.

g. When a CS learns that persons involved in an OIG case intend to commit or participate in a crime, or to cause harm to FDIC's programs and operations, the CS is encouraged to immediately notify the OIG contact or alternate.

h. No member of the OIG will disclose the identity of a CS without authorization from the Inspector General or designee, pursuant to the Inspector General Act of 1978, as amended (5 U.S.C., App. 3 §7(b)).

5. Procedures. The Assistant Inspector General who designates an individual as a confidential source, is responsible for ensuring that, once approved, a CS's identity remains confidential, and for following the procedures listed below:

a. Designating CS

(1) The Contact should direct a written request to the responsible Assistant Inspector General for authorization to designate an individual as a CS. If the written request is mailed, only registered mail or overnight mail should be used. The written request should include the full identity of the CS with as much background information concerning the individual as possible and a brief justification for using the individual as a CS. The procedures for recording hotline information (Paragraph 6. c.), outlined in our Hotline policy, *OIG Policies and Procedures Manual*, Chapter

110.3, satisfy these requirements. At most, only an original and one copy of the written request should exist; no copies should be maintained in the case files or workpapers. The responsible Assistant Inspector General should maintain the original and, if made, one copy placed in a locked safe or cabinet.

(2) If approved, a designation code that will be used to refer to the CS will be assigned. The designation code should identify the OIG office, followed by CS to note that the source is confidential and then a sequential number (e.g., G-CS-01 stands for the first CS in the Atlanta office of the OI.) The identifying information must be secured in a locked safe or cabinet and contain the true identity of the CS, designation code, case/assignment number, and contact's name.

b. Maintaining the Source's Confidentiality. CSs must not be identified by name, gender, or other telling information that may lead another to deduce a CS's true identity. Any reference to the CS should be by the designation code only. This applies to all written communication--from preparing internal papers (i.e., case files, work papers, etc.) to issuing relevant documents (i.e., reports, memorandum).

6. Contact. Questions regarding OIG guidance on this policy should be directed to the Assistant Inspector General for Management and Congressional Relations.