modification of the arrangement has certified that he or she:
(i) Is familiar with and will comply with the requirements of paragraph (a) of this section; and
(ii) Has no information of any violations or possible violations of paragraph (a) of this section, and will report immediately to the retained entity any subsequently gained information concerning a violation or possible violation of paragraph (a) of this section.

§ 31.217 Confidentiality of information.

(a) Nonpublic information defined. Any information that Treasury provides to a retained entity under an arrangement, or that the retained entity obtains or develops pursuant to the arrangement, shall be deemed nonpublic until the Treasury determines otherwise in writing, or the information becomes part of the body of public information from a source other than the retained entity.

(b) Prohibitions. The retained entity shall not:
(1) Disclose nonpublic information to anyone except as required to perform the retained entity’s obligations pursuant to the arrangement, or pursuant to a lawful court order or valid subpoena after giving prior notice to Treasury.
(2) Use or allow the use of any nonpublic information to further any private interest other than as contemplated by the arrangement.

(c) Retained entity’s responsibility. A retained entity shall take appropriate measures to ensure the confidentiality of nonpublic information and to prevent its inappropriate use. The retained entity shall document these measures in sufficient detail to demonstrate compliance, and shall maintain this documentation for three years after the arrangement has terminated. The retained entity shall notify the TARP Chief Compliance Officer in writing within five business days after detecting a violation of the prohibitions in paragraph (b) of this section. The security measures required by this paragraph shall include:
(1) Security measures to prevent unauthorized access to facilities and storage containers where nonpublic information is stored.
(2) Security measures to detect and prevent unauthorized access to computer equipment and data storage devices that store or transmit nonpublic information.
(3) Periodic training to ensure that persons receiving nonpublic information know their obligation to maintain its confidentiality and to use it only for purposes contemplated by the arrangement.
(4) Programs to ensure compliance with federal securities laws, including laws relating to insider trading, when the arrangement relates to the acquisition, valuation, management, or disposition of troubled assets.
(5) A certification from each key individual stating that he or she will comply with the requirements in this section, in the form of a nondisclosure agreement, before a key individual performs work under the arrangement, and then annually thereafter.

(d) Certification. No later than ten business days after the effective date of the arrangement, the retained entity shall certify to the Treasury that it has received a certification form from each key individual stating that he or she will comply with the requirements in §31.217(b). In making this certification, the retained entity may rely on the information obtained pursuant to paragraph (b) of this section, unless the retained entity knows or should have known that the information provided is false or inaccurate.

§ 31.218 Enforcement.

(a) Compliance with these rules concerning conflicts of interest is of the utmost importance. In the event a retained entity or any individual or entity providing information pursuant to 31 U.S.C. part 31 violates any of these rules, Treasury may impose or pursue one or more of the following sanctions:
(1) Rejection of work tainted by an organizational conflict of interest or a personal conflict of interest and denial of payment for that work.
(2) Termination of the arrangement for default.
(3) Debarment of the retained entity for Federal government contracting and/or disqualification of the retained entity.