

Recovery Accountability and Transparency Board

§ 200.16

any Board systems of records are informed of all requirements necessary to protect the privacy of individuals. The Board shall ensure that all employees having access to records receive adequate training in their protection and that records have adequate and proper storage with sufficient security to ensure their privacy.

(b) All employees shall be informed of the civil remedies provided under 5 U.S.C. 552a(g)(1) and other implications of the Privacy Act and of the fact that the Board may be subject to civil remedies for failure to comply with the provisions of the Privacy Act and the regulations in this part.

§ 200.14 Responsibility for maintaining adequate safeguards.

The Board has the responsibility for maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automated records systems. These security safeguards shall apply to all systems of records in which identifiable personal data are processed or maintained, including all reports and output from such systems of records that contain identifiable personal information. Such safeguards must be sufficient to prevent negligent, accidental, or unintentional disclosure, modification, or destruction of any personal records or data; must minimize, to the extent practicable, the risk that skilled technicians or knowledgeable persons could improperly obtain access to modify or destroy such records or data; and shall further ensure against such casual entry by unskilled persons without official reasons for access to such records or data.

(a) *Manual systems.* (1) Records contained in a system of records as defined in this part may be used, held, or stored only where facilities are adequate to prevent unauthorized access by persons within or outside the Board.

(2) Access to and use of a system of records shall be permitted only to persons whose duties require such access to the information for routine uses or for such other uses as may be provided in this part.

(3) Other than for access by employees or agents of the Board, access to records within a system of records

shall be permitted only to the individual to whom the record pertains or upon his or her written request.

(4) The Board shall ensure that all persons whose duties require access to and use of records contained in a system of records are adequately trained to protect the security and privacy of such records.

(5) The disposal and destruction of identifiable personal data records shall be done by shredding and in accordance with rules promulgated by the Archivist of the United States.

(b) *Automated systems.* (1) Identifiable personal information may be processed, stored, or maintained by automated data systems only where facilities or conditions are adequate to prevent unauthorized access to such systems in any form.

(2) Access to and use of identifiable personal data associated with automated data systems shall be limited to those persons whose duties require such access. Proper control of personal data in any form associated with automated data systems shall be maintained at all times, including maintenance of accountability records showing disposition of input and output documents.

(3) All persons whose duties require access to processing and maintenance of identifiable personal data and automated systems shall be adequately trained in the security and privacy of personal data.

(4) The disposal and disposition of identifiable personal data and automated systems shall be done by shredding, burning, or, in the case of electronic records, by degaussing or by overwriting with the appropriate security software, in accordance with regulations of the Archivist of the United States or other appropriate authority.

§ 200.15 Systems of records covered by exemptions.

The Board currently has no exempt systems of records.

§ 200.16 Mailing lists.

The Board shall not sell or rent an individual's name and/or address unless such action is specifically authorized by law. This section shall not be construed to require the withholding of

§ 200.17

4 CFR Ch. II (1-1-13 Edition)

names and addresses otherwise permitted to be made public.

§ 200.17 Exemptions.

(a) *General policy.* The Privacy Act permits an agency to exempt certain types of systems of records from some of the Privacy Act's requirements. It is the policy of the Board to exercise authority to exempt systems of records only in compelling cases.

(b) *Specific systems of records exempted under (j)(2) and (k)(2).* The Board exempts the RATB Investigative Files (RATB-11) system of records from the following provisions of 5 U.S.C. 552a:

(1) From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede the Board's criminal law enforcement duties.

(2) From subsection (c)(4) and (d) because notification would alert a subject to the fact that an open investigation on that individual is taking place, and might weaken the ongoing investigation, reveal investigatory techniques, and place confidential informants in jeopardy.

(3) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to the Board's close working relationship with other Federal, state and local law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(4) From subsection (e)(2) because collecting information to the fullest extent possible directly from the sub-

ject individual may or may not be practical in a criminal and/or civil investigation.

(5) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal and/or civil investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(6) From subsection (e)(4)(G)-(I) because this system of records is exempt from the access provisions of subsection (d).

(7) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(8) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(9) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual, which might in itself provide an answer to that individual relating to an ongoing investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(10) For comparability with the exemption claimed from subsection (f),