

**§ 102.33**

order and a description of the information disclosed. Notice shall not be given if disclosure is made from a criminal law enforcement system of records that has been exempted from the notice requirement.

(b) *Emergency disclosures.* Upon disclosing a record pertaining to an individual made under compelling circumstances affecting health or safety, the office shall notify that individual of the disclosure. This notice shall be mailed to the individual's last known address and shall state the nature of the information disclosed; the person, organization, or agency to which it was disclosed; the date of disclosure; and the compelling circumstances justifying the disclosure.

**§ 102.33 Security of systems of records.**

(a) Each Program/Support Office Head or designee shall establish administrative and physical controls to prevent unauthorized access to its systems of records, to prevent unauthorized disclosure of records, and to prevent physical damage to or destruction of records. The stringency of these controls shall correspond to the sensitivity of the records that the controls protect. At a minimum, each office's administrative and physical controls shall ensure that:

- (1) Records are protected from public view;
- (2) The area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to them;
- (3) Records are inaccessible to unauthorized persons outside of business hours; and
- (4) Records are not disclosed to unauthorized persons or under unauthorized circumstances in either oral or written form.

(b) Each Program/Support Office Head or designee shall establish procedures that restrict access to records to only those individuals within the SBA who must have access to those records in order to perform their duties and that prevent inadvertent disclosure of records.

(c) The OCIO shall provide SBA offices with guidance and assistance for privacy and security of electronic sys-

**13 CFR Ch. I (1-1-10 Edition)**

tems and compliance with pertinent laws and requirements.

**§ 102.34 Contracts for the operation of record systems.**

When SBA contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion of the record affected, are considered to be maintained by the SBA, and subject to this subpart. The SBA is responsible for applying the requirements of this subpart to the contractor. The contractor and its employees are to be considered employees of the SBA for purposes of the sanction provisions of the Privacy Act during performance of the contract.

**§ 102.35 Use and collection of Social Security Numbers.**

Each Program/Support Office Head or designee shall ensure that collection and use of SSN is performed only when the functionality of the system is dependant on use of the SSN as an identifier. Employees authorized to collect information must be aware:

- (a) That individuals may not be denied any right, benefit, or privilege as a result of refusing to provide their social security numbers, unless:
  - (1) The collection is authorized either by a statute; or
  - (2) The social security numbers are required under statute or regulation adopted prior to 1975 to verify the identity of an individual; and
- (b) That individuals requested to provide their social security numbers must be informed of:
  - (1) Whether providing social security numbers is mandatory or voluntary;
  - (2) Any statutory or regulatory authority that authorizes the collection of social security numbers; and
  - (3) The uses that will be made of the numbers.

**§ 102.36 Privacy Act standards of conduct.**

Each Program/Support Office Head or designee shall inform its employees of the provisions of the Privacy Act, including its civil liability and criminal penalty provisions. Unless otherwise permitted by law, an employee of the SBA shall:

## Small Business Administration

## § 102.39

(a) Collect from individuals only the information that is relevant and necessary to discharge the responsibilities of the SBA;

(b) Collect information about an individual directly from that individual whenever practicable;

(c) Inform each individual from whom information is collected of:

(1) The legal authority to collect the information and whether providing it is mandatory or voluntary;

(2) The principal purpose for which the SBA intends to use the information;

(3) The routine uses the SBA may make of the information; and

(4) The effects on the individual, if any, of not providing the information;

(d) Ensure that the office maintains no system of records without public notice and that it notifies appropriate SBA officials of the existence or development of any system of records that is not the subject of a current or planned public notice;

(e) Maintain all records that are used by the SBA in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination;

(f) Except as to disclosures made to an agency or made under the FOIA, make reasonable efforts, prior to disseminating any record about an individual, to ensure that the record is accurate, relevant, timely, and complete;

(g) Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity;

(h) When required by the Privacy Act, maintain an accounting in the specified form of all disclosures of records by the SBA to persons, organizations, or agencies;

(i) Maintain and use records with care to prevent the unauthorized or inadvertent disclosure of a record to anyone; and

(j) Notify the appropriate SBA official of any record that contains infor-

mation that the Privacy Act does not permit the SBA to maintain.

### § 102.37 Training requirements.

All employees should attend privacy training within one year of employment with SBA. All employees with Privacy Act responsibilities must attend Privacy Act training, whenever needed, that is offered by the SBA.

### § 102.38 Other rights and services.

Nothing in this subpart shall be construed to entitle any person, as a right, to any service or to the disclosure of any record to which such person is not entitled under the Privacy Act.

### § 102.39 SBA's exempt Privacy Act systems of records.

(a) Systems of records subject to investigatory material exemption under 5 U.S.C. 552a(k)(2), or 5 U.S.C. 552a(k)(5) or both:

(1) Office of Inspector General Records Other Than Investigation Records—SBA 4, contains records pertaining to audits, evaluations, and other non-audit services performed by the OIG;

(2) Equal Employment Opportunity Complaint Cases—SBA 13, contains complaint files, Equal Employment Opportunity counselor's reports, investigation materials, notes, reports, and recommendations;

(3) Investigative Files—SBA 16, contains records gathered by the OIG in the investigation of allegations that are within the jurisdiction of the OIG;

(4) Investigations Division Management Information System—SBA 17, contains records gathered or created during preparation for, conduct of, and follow-up on investigations conducted by the OIG, the Federal Bureau of Investigation (FBI), and other Federal, State, local, or foreign regulatory or law enforcement agency;

(5) Litigation and Claims Files—SBA 19, contains records relating to recipients classified as "in litigation" and all individuals involved in claims by or against the Agency;

(6) Personnel Security Files—SBA 24, contains records on active and inactive personnel security files, employee or former employee's name, background information, personnel actions, OPM,