

### § 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: