SBA

SOP 40 04 3

Privacy Act Procedures

Office of Hearings and Appeals

U.S. Small Business Administration

SMALL BUSINESS ADMINISTRATION
STANDARD OPERATING PROCEDURE

National

SUBJECT:	S.O.P.		REV
Privacy Act Procedures	SECTION 40	NO. 04	 3

INTRODUCTION

1. Purpose. To outline the procedures for the administration of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, and the Computer Matching Privacy Protection Amendments of 1990.

2. Personnel Concerned. All SBA Personnel.

3. SOP Canceled. SOP 40 04 2.

4. Originator. Freedom of Information/Privacy Acts Office, Office of Hearings and Appeals.

AUTHORIZED BY:		EFFECTIVE DATE
Delorice P. Ford Assistant Administrator Office of Hearings and Appeals		PAGE 1

SBA Form 989 (5-90) Ref: SOP 00 23

Table of Contents

Chapter 1

The Privacy Act and Computer Matching Privacy Protection Act

1. What is the Privacy Act of 1974?

The Privacy Act (PA) of 1974, Public Law 93-579 (5 U.S.C. § 552a), regulates the collection, maintenance, use, and dissemination of personal information by Federal agencies. The PA was amended by the Computer Matching Privacy Protection Act (CMPPA) of 1988 (P.L. 100-503, 5 U.S.C. § 552a(a)(8) - (13), (e)(12), (o), (p), (q), (r), and (u) (1994)), and the Computer Matching Privacy Protection (CMPPA) Amendments of 1990 (P.L. 101-56, 5 U.S.C. § 552a(p)). These amendments set forth computer matching activity requirements for Federal agencies.

2. What Safeguards Do the Privacy Act and the Computer Matching Privacy Protection Act Provide?

a. The PA provides safeguards for individuals against invasions of privacy by requiring Federal agencies, except as otherwise provided by law or regulation, to:

(1) Permit individuals to know what records pertaining to them are collected, maintained, used, or disseminated;

(2) Allow individuals to prevent records pertaining to them, obtained for a particular purpose, from being used or made available for another purpose without their consent;

(3) Permit individuals to gain access to information pertaining to them, obtain a copy of all or any portions thereof, and correct or amend such records;

(4) Collect, maintain, use, or disseminate personally identifiable information in a manner that ensures the information is current and accurate, and that adequate safeguards are provided to prevent misuse of such information;

(5) Permit exemption from the requirements of the Act only where an important public policy need exists as determined by specific statutory authority; and

(6) Be subject to a civil suit for any damages that occur as a result of action that violates any individual's rights under this Act.

b. The CMPPA amended the PA regarding the use of automated PA records for Federal, State, and local computer matching. Its purpose is to ensure privacy, integrity, and verification of data disclosed by monitoring for the following:

(1) Procedural uniformity. Agencies must comply with the Act's specific matching procedures.

(2) Due process for subjects. The Act provides due process rights including advance notice that records may be matched, notice of any adverse data found, and opportunity for rebuttal.

(3) Oversight of matching. Oversight compliance includes reports to the Office of Management and Budget (OMB) and Congress, public notices in the Federal Register, and establishment of Data Integrity Boards (DIB).

3. Which Small Business Administration Officials Have Privacy Act Responsibilities?

a. The Assistant Administrator for Hearings and Appeals is the Senior Official for Privacy Policy, designated by the Administrator, and has primary responsibility for privacy policy issues on a national level.

b. The PA Officer, who is the Chief, Freedom of Information/Privacy Acts (FOI/PA) Office, is responsible for overseeing and implementing the Act, and:

(1) Reviews and makes final Small Business Administration (SBA) decisions on PA appeals seeking amendment and access to records;

(2) Monitors the relevancy, accuracy, and completeness of records contained in systems of records;

(3) Prepares reports as required to OMB (see Chapter 9-3), the Attorney General, and the President;

(4) Prepares rules and notices for publication in the Federal Register;

(5) Develops PA training programs for SBA personnel; and

(6) Develops materials such as forms, reporting formats, and directives for implementing the PA.

(7) Oversee the Agency's FOIA Database which also is used to records all PA cases (see Chapter 9).

(8) Monitor and assist with all of the Agency's Privacy Impact Assessment (PIA) Statements (see Chapter 9).

c. Systems Manager. The senior official in all SBA field and program offices will designate a Systems Manager, whose PA responsibilities for that office are to:

(1) Maintain appropriate records and ensure security (see chapter 6);

(2) Review records for relevancy, timeliness, completeness, and accuracy;

(3) Be the initial point of contact for individuals seeking access to or amendment of their records;

(4) Act on requests when the records are located in that office;

(5) Forward requests to the office where the records are located;

(6) Inform requesters of estimated fees and collect fees (see paragraph 4-4); and

(7) Collect and compile information for reports, PIAs and Federal Register notices.

(8) Ensure that all PA cases are entered into the FOIA Database.

4. What Terms are Commonly Used in the Privacy Act?

a. Agency is any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the executive branch of the Federal Government (including the Executive Office of the President), or any independent regulatory agency.

b. Federal benefit program is any program administered or funded by any agent or State on behalf of the Federal Government, that provides cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

c. Federal personnel are officers and employees of the Government of the United States, members of the uniformed services, and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the U.S. Government.

d. Individual is a citizen of the United States or an alien lawfully admitted for permanent residence. This term does not include entrepreneurial enterprises (e.g., sole proprietors, partnerships, corporations, or other forms of business entities).

e. Maintain is to maintain, collect, use, or disseminate.

f. Matching program is any computerized comparison of:

(1) Two or more automated systems of records or a system of records with non-Federal records for the purpose of:

(a) Establishing or verifying information with respect to cash or in-kind assistance or payments under Federal benefit programs; or

(b) Recouping payments or delinquent debts under such Federal benefit programs; or

(2) Two or more automated Federal personnel or payroll systems of records; or

(3) A system of Federal personnel or payroll records with non-Federal records.

g. Non-Federal agency is any State or local government, or agency thereof, that receives records contained in a system of records from a source agency for use in a matching program.

h. Recipient agency is any agency, or its contractor, that receives records contained in a system of records from a source agency for use in a matching program.

i. Record is any item, collection, or grouping of information about an individual that an agency maintains including education, finances, medical history, criminal or employment history, and that contains the individual's name, identifying number, symbol, or other identifying mark, such as a finger or voice print, or a photograph.

j. Routine use, with respect to the disclosure of a record, is the use of a record for a purpose compatible with the purpose for which it was collected.

k. Source agency is any agency or any State or local government or agency that discloses records contained in a system of records to be used in a matching program.

l. System of records is a group of any records under SBA's control containing information that is retrievable by an individual's name or identifying number, symbol, or other identifying personal characteristic. The SBA Home Page at www.sba.gov/gils/ lists the SBA's systems of records.

5. What is the Relationship Between the Privacy Act and the Freedom of Information Act?

a. The Freedom of Information Act (FOIA) 5 U.S.C. § 552, (see SOP 40 03), permits any person to request any agency record and requires Federal agencies to disclose all agency records unless information is protected by any of the nine statutory exemptions of the FOIA. In contrast, the PA permits individuals to seek access to their own records if those records are maintained within an agency's

system of records and retrieved by the requester's own name or personal identifier. Nothing in the PA limits public access granted under the FOIA. The two Acts should not conflict, since the FOIA exemptions are designed to prevent an invasion of privacy.

b. The FOIA and the PA interact in two distinct areas.

(1) First-Party Access - SBA must consider the FOIA, as well as the PA, whenever individuals request access to their own records contained in a system of records.

(2) Third-Party Access - SBA must consider the PA when a person makes a FOIA request for another individual's records that are contained in a system of records. The PA limits a third party's FOIA right of access to another individual's PA protected records.

6. What Categories of Materials are not Subject to the Privacy Act?

a. The following are not subject to PA provisions.

(1) Personal notes in the sole possession of the author, that are retained or discarded at the author's discretion and which the SBA does not control.

(2) Files in the sole possession and exclusive use of one individual (e.g., personal telephone lists, mailing lists, personal incident notes, etc.). (Note: If the file becomes part of the office or activity and circulates within the SBA, it will be subject to the PA provisions.)

b. Records of companies, corporations, partnerships, and sole proprietorships.

c. Records not retrievable by an individual's name or other personal identifier.

7. What Must be Considered When SBA Collects Information About Individuals?

a. Relevancy. Collect only information that is relevant and necessary to the SBA's mission in order to avert potentially harmful disclosures.

b. Accuracy. Ensure that all information collected is accurate when determining an individual's rights, benefits, or privileges on the basis of that information.

c. Informing individuals. Notify individuals of the following.

(1) The legal authority (whether granted by statute or by Presidential Executive Order) for collection of the information in each of SBA's

systems of records is listed in that system. See SBA's Systems of Records at www.sba.gov/gils/.

(2) The principal reason. Explain the purpose(s) for which the SBA will use the information.

(3) The routine uses. A published notice in the Federal Register lists the SBA's systems of records and routine uses (also see www.sba.gov/gils/).

(4) The requested disclosure of an individual's Social Security Number (SSN). SBA will inform the individual whether disclosure is mandatory (and under what authority) or voluntary. Rights, benefits, or privileges provided by law cannot be denied because of refusal to disclose a SSN unless:

(a) Disclosure is required by Federal statute; or

(b) Disclosure is for a system of records in existence and operation prior to January 1, 1975, if disclosure was required under statute or regulation adopted prior to that date to verify the individual's identity.

(5) The effect of nondisclosure. If information being collected is relevant and necessary for the SBA's duties and individuals refuse to provide it, the SBA must inform them of the consequences of refusal.

8. Which SBA Forms and Records Must Contain Privacy Act Language?

a. All standard operating procedures (SOP) dealing with the collection, maintenance, use, and dissemination of personal information must contain a reminder of PA responsibilities.

b. All forms that request an SSN must contain language as to the authority and use of the SSN and whether collection is mandatory or voluntary as discussed in paragraph 1-7.c.(4) above.

9. What are the Privacy Act Requirements Regarding Accurate Records?

All SBA records concerning individuals must be accurate, relevant, timely, and complete to ensure fairness to all.

10. Should Records be Maintained on How Individuals Exercise First Amendment

Rights?

No, do not keep such records. These rights include religious and political beliefs, freedom of speech and the press, and freedom of assembly and to petition.

Chapter 2

Disclosures

1. What are the Conditions for Disclosure of Records Maintained in a Privacy Act System of Records?

The SBA will not disclose any record that is contained in a system of records to any person or to another agency, except pursuant to a written request by, or with the written consent of, the individual to whom the record pertains, unless such disclosure is:

a. To SBA employees, volunteers, interns, expert witnesses and contractors who have an official need for the record (See Chapter 7);

b. Required under the FOIA;

c. For an established routine use of the record;

d. To the Bureau of Census for a census, survey, or related activity;

e. To a recipient who has provided the SBA with adequate written assurance that it will be used solely for statistical research or as a reporting record, in which case, you should transfer the record in a form that is not individually identifiable;

f. To the National Archives and Records Administration (NARA) because the record has sufficient historical or other value to warrant preservation by the Government, or to the General Services Administration (GSA) for determination of the record's historical or other value;

g. To another agency or agent of a Government jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, in which case, the request must specify the particular portion of the record desired and the law enforcement activity for which the record is sought;

h. In an emergency affecting the health and safety of an individual, in which case, you should notify the individual of such disclosure at the last known address;

i. To either House of Congress, or any committee, or subcommittee thereof that has proper jurisdiction;

j. To the General Accounting Office (GAO) for official duties;

k. Pursuant to a court order from a court of competent jurisdiction; or

l. To a consumer reporting agency in accordance with section 3711(e) of Title 31, U.S.C.

2. How Does the SBA Account for Disclosures and Amendment of Records?

a. For each system of record, SBA will keep an accurate accounting of each disclosure (except for disclosures under paragraphs 1.a. and 1.b. of this chapter) and of each request for amendment.

b. The Systems Manager must account for disclosures and requests for amendment in the following manner.

(1) Maintain the accounting for 5 years or the life of the record, whichever is longer.

(2) Except for disclosures made under paragraphs 1.a., 1.b., and 1.g. of this chapter, make the accounting available to individuals named in the record at their request.

(3) Retain copies of pertinent correspondence (include name and address of the person or agency to whom the disclosure is made) for at least 5 years.

3. Can Systems Managers Consult with Other SBA Offices Prior to Disclosure and/or Amendment of Privacy Act Records?

Yes. Systems Managers may consult the FOI/PA Office for technical assistance; the Office of General Counsel (OGC) for a legal opinion; or with any other SBA officials who have relevant knowledge.

Chapter 3

Privacy Act Exemptions

1. What are the Privacy Act Exemptions and What Types of Records Do They Protect?

a. The Act provides one "special" exemption, 5 U.S.C. § 552a(d)(5), that protects information compiled in reasonable anticipation of a civil action or proceeding. The exemption also extends to information prepared in anticipation of quasi-judicial administrative hearings. The provision is similar to the attorney work-product privilege encompassed by Exemption 5 of the FOIA, and may protect information prepared by a non-attorney.

b. Two general exemptions are:

(1) 5 U.S.C. § 552a(j)(1) – protects records maintained by the Central Intelligence Agency; and

(2) 5 U.S.C. § 552a(j)(2) – covers records maintained by an agency that performs, as its principal function any activity pertaining to the enforcement of criminal laws and consisting of:

(a) Information compiled to identify criminal offenders and alleged offenders and consists only of identifying data and notations of arrests, confinement, release, and parole or probation status;

(b) Information, including reports of informers or investigators, associated with an identifiable individual compiled to investigate criminal activity; or

(c) Reports, compiled at any stage of the process, of enforcement of criminal laws from arrest or indictment through release from supervision if those reports are associated with an identifiable individual.

In accordance with this Exemption, the Agency promulgated the following systems of records to protect records compiled for criminal law enforcement purposes: Audit Reports, Personnel and Security Files, Security and Investigations Files, Office of Inspector General Referrals, and Investigations Division Management Information System.

c. The seven specific exemptions are:

(1) 5 U.S.C. § 552a(k)(1) – protects records subject to Exemption 1 of the FOIA (5 U.S.C 552(b)(1))(National Security issues);

(2) 5 U.S.C. § 552a(k)(2) – covers investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) above, provided, however, that if any individual is denied any right, privilege, or benefit that he/she would otherwise be entitled by Federal law, or for which he/she would be eligible, as a result of the maintenance of such material, such material must be provided to such individual, except to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality, or prior to the effective date of 5 U.S.C § 552a (9/27/75), under an implied promise of confidentiality;

(3) 5 U.S.C. § 552a(k)(3) – certain Secret Service record systems pursuant to section 3056 of Title 18, U.S.C.;

(4) 5 U.S.C.§ 552a(k)(4) – protects information "required by statute to be maintained and used solely as statistical records;"

(5) 5 U.S.C. § 552a(k)(5) – generally applicable to source-identifying material in background employment and personnel-type investigative files, to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality, or prior to the effective date of 5 U.S.C. § 552a (9/27/75), under an implied promise of confidentiality;

(6) 5 U.S.C. § 552a(k)(6) – protects testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process; and

(7) 5 U.S.C. § 552a(k)(7) – covers evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality, or prior to the effective date of this section (9/27/75), under an implied promise of confidentiality.

Chapter 4

Access to and Amendment of Records

1. What Access and Amendment Procedures Does the Privacy Act Provide?

a. Rights of Access and Amendment.

Individuals may request:

(1) access to their records or any information pertaining to them which is contained in any of SBA's system of records; and

(2) amendment of a record pertaining to them when they believe the record is not accurate, relevant, timely, or complete.

b. Requests for Access or Amendment.

(1) Access or amendment requests must be made in writing to the appropriate Systems Manager or to the PA Officer, 409 Third Street, SW, Washington, DC 20416, who will direct the request to the proper SBA official.

(2) The request must contain a reasonable description of the SBA system(s) of records where the information may be found, and must include a notarized affidavit or a signed declaration of the individual's identity. The Systems Manager (or, when appropriate, the PA Officer) will respond in writing and may ask for more specific information or for further identification.

(3) When an individual submits a PA request by electronic mail, SBA will not process the request until it receives proof of identity with an original signature.

c. Disclosures to Representatives.

(1) Individuals may request that:

(a) A person of their own choosing be allowed to accompany them during the review of a record; or

(b) Their record be released to their representative who must present a written consent from the individual prior to release.

(2) The Systems Manager may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

d. SBA Responsibilities.

(1) Upon receipt of a request for access or amendment, the Systems Manager must notify the requester in writing within 10 working days whether the request will be granted or denied.

(2) If the request for access is granted, the notification should state:

(a) that unless the requester objects for good cause, the record will be mailed; or

(b) the time and place where the record may be reviewed.

(3) If the request for amendment is granted, the Systems Manager must promptly correct any portion of the record that the individual believes is not accurate, relevant, timely, or complete. The Systems Manager must provide a copy of the amended record to prior recipients of the record.

(4) The Systems Manager must notify individuals denied the right of access or amendment of the reasons for denial and their right to appeal the decision to the PA Officer, 409 Third Street, SW, Washington, DC 20416. All appeals of denials must be submitted within 30 working days of the denial or within 90 working days if the appeal is for the failure to make a determination. The appeal should specify the reasons for requesting a review and must be accompanied by affidavits, statements, or other supporting material justifying the appeal.

2. What is the SBA's Privacy Act Appellate Procedure?

a. The PA Officer will consider all relevant material, including the System Manager's decision, and the material submitted by the requesting individual. The PA Officer may consult with OGC for a legal opinion and other SBA officials who have relevant knowledge.

b. The PA Officer must issue a final decision no later than 30 working days after receipt of an appeal, unless the 30-day period is extended for good cause. If so, the PA Officer must notify the individual of the expected response date.

c. If the PA Officer denies access or amendment, he/she must:

(1) Notify the individual of the reason for the denial;

(2) Notify the individual of their right to judicial review;

(3) Allow the individual to file a concise statement explaining their reasons for disagreement if an amendment appeal is denied; and

(4) Mark the areas of dispute, include the individual's statement of disagreement in the file, and if appropriate, a statement of why SBA refused to amend the record. The PA Officer must provide a copy of this material to prior recipients of the record.

d. If the PA Officer grants access or amendment to file:

(1) For access to a file, the PA Officer will notify the individual:

(a) that, unless the individual objects for good cause, the record will be mailed; or

(b) provide the time and place where the record may be reviewed.

(2) For amendment of a file, the PA Officer will promptly correct any portion of the record that the individual believes is not accurate, relevant, timely, or complete. The PA Officer must provide a copy of the amended record to prior recipients of the record.

e. Nothing in 5 U.S.C. § 552a shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

3. What is the SBA's Privacy Act Appellate Procedure Concerning Records Contained in Office of Personnel Management (OPM) and Equal Employment Opportunity Commission (EEOC) Systems of Records?

a. Appeals for records contained in OPM's Government-wide Systems of Records, OPM/GOVT-1 - OPM/GOVT-10, must be sent to the Assistant Director for Workforce Information Personnel Systems and Oversight Group, OPM, 1900 E Street, NW, Washington, DC 20415.

b. Appeals for records contained in EEOC's Government-wide System of Records, EEOC/GOVT-1, must be sent to the Legal Counsel, EEOC, 1801 L Street, NW, Washington, DC 20507.

4. What Fees Will the SBA Charge to Process a Privacy Act Request?

SBA will not charge for the first copy of an individual's Official Personnel File. Thereafter, SBA will charge $.10/page for copies. SBA will waive fees of $25.00 or less.

Chapter 5

Computer Matching Program Procedures

1. What Procedures are Required by the Computer Matching Privacy Protection Act?

a. Matching agreements. No record contained in a system of records may be disclosed to a recipient or non-Federal agency for a computer matching program without a written agreement between the source, recipient, or non-Federal agency. The agreement must specify:

(1) The purpose and legal authority for conducting the program;

(2) The justification for the program and anticipated results, including a specific estimate of savings;

(3) A description of the records including each data element, approximate number of records, and projected starting and completion dates;

(4) Procedures for providing individualized notice at the time of application and notice periodically thereafter as directed by the Data Integrity Board (DIB) to:

(a) Applicants for and recipients of financial assistance or payments under Federal benefit programs; and

(b) Applicants for and holders of Federal positions that information provided above may be subject to verification through matching programs;

(5) Procedures for verifying information produced in a matching program as paragraph c. below requires;

(6) Procedures for the retention and destruction of identifiable records created in a matching program by a recipient or non-Federal agency;

(7) Procedures for ensuring the administrative, technical, and physical security of the records matched, and for program results;

(8) Prohibitions on duplication and re-disclosure of records provided, except where required by law or essential to the conduct of the matching program;

(9) Procedures for the use, return, or destruction of records provided in a matching program;

(10) Information on assessing the accuracy of the records to be used; and

(11) The Comptroller General (CG) may have access to all records of a recipient or non-Federal agency that the CG deems necessary to monitor or verify compliance with the agreement.

b. Agreement specifications. A copy of each agreement described above will be provided to the Senate Committee on Governmental Affairs, the House Committee on Governmental Operations, and the public upon request.

(1) Agreements will be effective 30 days after the date a copy is provided.

(2) An agreement shall remain in effect only for a period, not to exceed 18 months, that the DIB determines is appropriate for its purpose, and the time necessary to conduct the matching program.

(3) Within 3 months prior to the expiration of an agreement, the DIB may, without additional review, renew the matching agreement for no more than 1 additional year if:

(a) The program will be conducted without any change; and

(b) Each party to the agreement certifies to the DIB in writing that the program complies with the agreement.

c. Verification. To protect an individual whose records are used in matching programs, no participant agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to the individual, or take adverse action against the individual as a result of information produced by matching programs, until the information has been independently verified.

(1) Independent verification requires separate investigation and confirmation of information used as a basis for an adverse action against an individual including, where applicable:

(a) The amount of the asset or income involved;

(b) Whether the individual actually has or had access to the asset or income for personal use; and

(c) The period(s) when the individual actually had the asset or income.

(2) No participant agency may suspend, terminate, reduce, or make a final determination denying any financial assistance or payment under a Federal benefit program, or take adverse action as a result of information produced

by a matching program:

(a) Unless the individual has received notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest the findings; and

(b) Until the expiration of any notice period provided by the program's law or regulations, or 30 days, whichever is later. An opportunity to contest may be satisfied by notice, hearing, and appeal rights governing a Federal benefit program. The exercise of those rights shall not affect rights available under this paragraph.

(3) An agency may take appropriate action otherwise prohibited by paragraph 1.c.(2)(b) of this chapter if the agency determines that public health or safety may be adversely affected or significantly threatened during the notice period required by such paragraph.

d. Sanctions. Notwithstanding any other law, a source agency may not disclose a record from a system of records for a matching program to a recipient or non-Federal agency if the source agency has any reason to believe that the above requirements, or any matching agreement entered into pursuant to paragraph 1.b. of this chapter, or both, are not being met by the recipient agency. No source agency may renew a matching agreement unless:

(a) The recipient or non-Federal agency has certified it has complied with the provisions of that agreement; and

(b) The source agency believes the certification is accurate.

e. Data Integrity Board. Agencies that conduct or participate in matching programs must establish a DIB to oversee and coordinate the program. Members of the SBA DIB include senior officials designated by the Administrator, including the IG (who may not serve as Chair) and the Assistant Administrator for Hearings and Appeals, who is the senior official responsible for the implementation of the PA. The DIB must:

(1) Review, approve, and maintain all written agreements for receipt or disclosure of SBA records for matching programs;

(2) Review all matching programs in which the SBA has participated during the year; determine compliance with applicable laws, regulations, guidelines, and agency agreements; and assess the costs and benefits of the programs;

(3) Review all recurring matching programs in which the SBA has participated during the year for continued justification of disclosures;

(4) Compile a biennial report to the Administrator and OMB, that is available to the public upon request, describing the SBA's matching activities, including:

(a) Matching programs in which the SBA has participated;

(b) Matching agreements proposed that were not approved by the DIB;

(c) Change in membership or structure of the DIB in the preceding year;

(d) Reasons for any waiver of the requirement described below for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(e) Violations of matching agreements that have been alleged or identified, and corrective action taken; and

(f) Other information required by OMB to be included in the report;

(5) Serve as clearinghouse for the completeness, accuracy, and reliability of records used;

(6) Interpret and guide SBA components and personnel on the requirements for matching programs;

(7) Review SBA record-keeping policies and practices for matching programs to ensure compliance; and

(8) Review and report on any SBA matching activities that are not matching programs.

f. Cost-benefit analysis. Except as provided in paragraphs e.(2) and (3) above, the DIB must not approve any written agreement for a matching program unless the SBA has submitted to the DIB a cost-benefit analysis of the proposed program demonstrating the cost-effectiveness. The DIB may waive these requirements if, consistent with OMB guidelines, a cost-benefit analysis is not required. An analysis is not required prior to the initial approval of a written agreement for a matching program that is specifically required by statute.

g. Disapproval of matching agreements. If a matching agreement is not approved by the DIB, any party to the agreement may appeal to OMB. OMB will notify the Senate Committee on Governmental Affairs and the House Committee on Government Operations of the appeal.

(1) OMB may approve a matching agreement despite the disapproval of the DIB if OMB determines that:

(a) The matching program complies with all applicable legal, regulatory, and policy requirements;

(b) Adequate evidence exists that the matching agreement will be cost-effective; and

(c) The matching program is in the public interest.

(2) The decision of OMB to approve a matching agreement must not take effect until 30 days after it is reported to the committees described above.

(3) If the DIB and OMB disapprove a matching program proposed by the IG, the IG may report the disapproval to the Administrator and to Congress.

h. Reports. OMB will prepare a biennial report to Congress that consolidates information reported from the various DIBs. The report will detail the costs and benefits of matching programs conducted during the report period, and identify each waiver of the required submission of a cost-benefit analysis granted by a DIB, and the reasons for granting the waiver. In order to protect ongoing law enforcement or counter-intelligence operations, SBA may report non-matching activities on an aggregate basis.

Chapter 6

Security of Records

1. Does the Privacy Act Provide Guidelines for the Maintenance of Records?

a. Yes. All persons involved in the design, development, operation, or maintenance of a system of records must abide by the SBA's rules of conduct and be aware of the PA's penalties for noncompliance. The Office of Chief Information Officer (OCIO) maintains the SBA's automated data and formulates security policy for automated systems.

b. Administrative, technical, and physical safeguards must be established to ensure the security, confidentiality, and protection of information maintained.

c. When identifiable personal data subject to the PA is not under the personal control of authorized personnel, all such information must be stored in a locked file, desk, card cabinet, or receptacle. Each affected office must establish procedures to ensure proper storage and security, and must designate an individual responsible for these duties. Lock all storage cabinets at the end of each day. Alternate storage systems may be used if they furnish equivalent or greater physical security.

2. What Other Provisions Exist for Computer Security?

a. Federal Information Processing Standards (FIPS PUB 41) dated May 10, 1975, apply to computer security. The procedures described above are minimal and may be expanded or substituted as long as automated personal data is not compromised.

b. The Computer Security Act of 1987. Public Law 100-235 establishes a computer standards program within the National Institute of Standards and Technology (NIST) to provide Government-wide guidelines on computer security. It requires Federal agencies to identify and develop an inventory of systems that contain sensitive information, and to provide training in security matters to persons involved in the management, operation, and use of Federal computer systems.

c. SOP 90 47 - Automated Information Security Program. Establishes SBA's overall policies and procedures for ADP security as required by the Computer Security Act and OMB Circular A-130.

d. Section 208 of the E-Government Act of 2002 (P.L. 017-347, 44 USC Ch. 36). Establishes Government-wide procedures for the reviews of how information about individuals is handled within agencies when they use information technology (IT) to collect new information, or when agencies develop or buy new

IT systems to handle collections of personally identifiable information. All Agencies must conduct a Privacy Impact Assessment (PIA) for electronic information systems and collections and must make them publicly available.

(1) A PIA is an analysis of how information is handled:

(a) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(b) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and

(c) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

(2) The SBA Office that will use and maintain the collection of information is responsible for preparing the PIA. The Office of the Chief Information Officer must approve the PIA. An electronic copy will be forwarded to the FOI/PA Office and will be made electronically available to the public on the FOI/PA home page. A copy will also be forwarded to OMB. (See paragraph 9-3).

3. How are Records Secured?

a. Limit access to records that contain personal data to persons who are required to use the data in the performance of their duties, or have a demonstrated need to know the contents of a specific file.

b. Destroy products, records, or source documents that are obsolete so that the data cannot be recovered or reconstructed.

c. Assign an individual in each office to examine the effectiveness of the administrative, technical, and physical controls.

d. Establish a system to satisfy the disclosure, access, and amendment reporting requirements of the PA.

4. How are Automated Records Secured?

a. Information Management Practices.

(1) Handling of Personal Data.

(a) Take precautions to ensure that unauthorized personnel cannot access personal information. Secure computerized personal data. Hand-carry completed computer runs and data to the responsible control clerk. Prepare a list of authorized individuals for access control, authorization validation, and to oversee movement of personnel within the facility. Restrict all other personnel to areas where personal data is not stored.

Any employee who knowingly discloses personal data to an unauthorized person or agency is subject to criminal sanctions.

(b) Distribution of computer products containing personal data is limited to persons required to use the data or who need to know the contents of a specific data file. To ensure conformity with the PA, prepare a hard copy list of personnel authorized to receive computer products from each separate automated system of records. No product containing personal data will be distributed, displayed, or disseminated to unauthorized personnel.

(c) Upon expiration of the retention date, destroy all cards, rosters, and other listings that contain personal data using a method that ensures the data cannot be recovered or reconstructed.

(2) Assignment of Responsibilities.

(a) Assign an individual to examine the effectiveness of storage, use, and processing practices. Responsibilities include: evaluation of physical security, information management practices and computer system access controls; consideration of internal uses and authorized external transfer of data; and recommendations to management of ways to eliminate risks or violations.

(b) Designate a responsible official for the protection and accountability of all personal data in automated systems where identifiable personal data is processed, stored, or maintained.

b. Physical Security.

(1) Disaster Recovery.

Develop fire protection and disaster recovery procedures to ensure that all personal data can be recovered. Include instructions for removal of critical stored data to a safe vicinity outside the immediate computer facility. This remote location must be able to protect the critical files adequately. Disaster recovery procedures should be tested periodically.

(2) Access Control.

Monitor and control the movement of material around the computer room and related areas. Limit to authorized personnel, access to conversion, ADP processing, and data control areas. Store computer-generated output products in adequate containers in a secured room.

(3) Storage Protection.

Store files (tape or disk) containing personal data in a vault which has a certified protection rating and which protects the contents from steam, water damage, heat, and fire.

(4) Training and Orientation.

Establish rules of conduct for computer personnel. Develop training to inform persons involved in media conversion, data control, and the preparation and processing of computer products of their responsibilities under the PA.

(5) Security Inspection.

Conduct periodic unannounced security inspections to evaluate security measures. At a minimum, ensure that doors are locked, locks are in good working order, and fire and intrusion alarms activated.

c. Computer System Security Controls.

(1) Access Controls.

(a) Verify authorized use of data by preparing an inventory of current programs which process or access personal data. Enforce programming practices and include audit trails. Prepare written guidelines relating the stringency of testing to the magnitude of the data, and tailor them to the ADP facility. Require strict controls and written authorizations for all operating system changes involving software security. Document procedural controls over data, operations, system design, programming, and acceptance testing. See paragraphs 6-1 and 6-2 above.

(b) Maintain strict controls over programming language and other computer access and control media. Preparation, control, and use of all input and control media is the responsibility of the unit assigned to operate the computer facility. System and software support personnel who use programming language and other computer accesses and controls, are authorized to use all means at

their disposal to edit, access, and control the operating system, research program and/or operating system problems, but only to the extent necessary to ensure efficient and effective data processing activities. All activities of systems support personnel must be strictly monitored and controlled by the head of the system software support unit.

(2) Access Auditing.

Develop procedures for identification of system users and routine uses of data files. Initiate procedures to account for the disposition of personnel data.

5. How are Communications Systems Secured?

a. Locate all remote terminals in a secure area (SBA personnel access only). All manuals and other materials relating to the operation of the terminal will be locked in a metal file cabinet or any other equally secure storage area.

b. Limit network access to personal records. Establish classes of authorized users to perform specific activities and store this information in the computer, or use read/write key protection; or a combination of these or other methods.

c. Maintain transmission logs of storage media and terminal activity, requirements identification, access control, and audits of network activity.

Chapter 7

Other Provisions of the Privacy Act

1. Who is Responsible for Changing and Publishing System Revisions?

Systems Managers are responsible for making changes and additions to any system of records affecting their offices. They must publish the revised system in the Federal Register after receiving approval from the FOI/PA Office. OMB requires 30 days notice in the Federal Register of any proposal to establish or alter any systems of records. OMB Circular A-130 specifies that major changes or new systems must be reported to OMB and Congress.

2. What Privacy Act Considerations Apply to Agency Expert Witnesses, Contractors, Volunteers, or Interns?

SBA contractors, volunteers, and interns are required to comply with the Privacy Act. SBA will not release PA information to a contractor, volunteer, or intern unless there is an appropriate routine use or after consulting with the FOI/PA Office. SBA must inform contractors, volunteers, and interns of this duty to comply with the PA and instruct them regarding the use and maintenance of a PA system. SBA must counsel all contractors, volunteers, and interns that they must continue to protect the confidentiality of PA information even after completion of their tenure with the Agency.

The PA does not cover records kept by a contractor for its own purposes (e.g., its personnel records).

3. Are Mailing Lists of Individuals Releasable?

SBA must not release, sell, or rent an individual's name or address. SBA must release names or addresses that are otherwise made public, such as the names of borrowers.

4. Who Can Represent an Individual?

The custodial parent of any minor, or the legal guardian of any individual who has been declared by a court of competent jurisdiction to be incompetent due to physical or mental capacity or age, may act on behalf of the individual.

5. Does the SBA Maintain Systems of Records Belonging to Other Agencies?

a. Yes. As prescribed by OPM, the SBA maintains Official Personnel Files, as well as those described in OPM's Government-wide systems of records. The SBA

must protect the privacy of all individuals concerned, in accordance with OPM regulations.

b. The SBA Office of Equal Employment Opportunity and Civil Rights Compliance maintains files belonging to the EEOC and subject to the systems described in EEOC/ GOVT-1.

6. Are Individuals Required to Provide Their Social Security Numbers?

The SBA must not require an individual to disclose his or her SSN unless specifically authorized by statute and must not deny any right, benefit, or privilege provided by law because of a refusal to disclose. If SBA requests individuals to disclose their SSNs, SBA must inform them whether disclosure is mandatory or voluntary; if the former, by what statutory or other authority the number is solicited, and what uses will be made of it. See paragraph 1-7.c.(4).

Chapter 8

Civil and Criminal Actions

1. Judicial Review of Privacy Act Violations.

a. The PA authorizes judicial review in Federal District court for the following agency actions:

(1) Refusal to grant access;

(2) Refusal to amend or correct a record;

(3) Failure to maintain a record with accuracy, relevancy, timeliness, or completeness as is necessary to assure fairness in a determination made on the basis of such record where an adverse determination results; and

(4) Failure to comply with any other provision of the Act, or any rule promulgated thereunder, where there is an adverse affect on the individual.

b. Individuals may pursue the above matter(s) in United States District Court in the district in which they reside, or have a principal place of business, or where the records are located, or in the District of Columbia.

c. If a court determines the SBA is liable, SBA must provide to the individual:

(1) The damages sustained as a result of the SBA's action. If less than $1,000, the individual shall receive the sum of $1,000; if more than $1,000, the SBA shall be liable for the exact amount.

(2) The costs of the lawsuit, as well as reasonable attorney's fees, estimated by the court.

2. Criminal Penalties.

a. An SBA employee can be found guilty of a misdemeanor where that employee knowingly and willfully:

(1) Discloses records to an unauthorized party; or

(2) Maintains a system of records without publishing a public notice.

b. Fraudulent representation by an individual to obtain another individual's record is punishable as a misdemeanor and subject to a maximum fine of $5,000.

Chapter 9

Notices, Reports and Database

1. Notices of Systems of Records.

The SBA must publish a notice in the Federal Register when it establishes a new system or changes an existing system. The SBA must submit a report on these systems to OMB and to Congress. See paragraph 7-1.

a. The Systems Manager, with the approval of the PA Officer, will submit changes for publication. If the entire system of records is affected, the PA Officer is responsible for publication. Changes may include:

(1) A new routine use;

(2) Changes in or expansion of categories of individuals;

(3) Changes in or expansion of categories of records;

(4) Change in the SBA's rules for notifying individuals that their records are maintained, or changes in access, amendment, or appeal procedures; or

(5) A system is revised or deleted.

2. Biennial Report.

The PA Officer will prepare and submit a biennial report to OMB in accordance with their instructions. This report is a SBA-wide summary and will include the following information:

a. Numbers of times access or amendment to records was requested, granted, or denied;

b. Numbers of appeals resulting from denial of access or amendment to records, and numbers granted or denied;

c. Numbers of exempt and non-exempt systems;

d. Numbers and results of PA court actions;

e. Information on matching programs, as described in chapter 5; and

f. Other information required by OMB, which may include accomplishments, plans,

and operational experiences.

3. What is a Privacy Impact Assessment Statement?

See paragraph 6-2 (d).

4. What is the FOIA Tracking System?

The FOIA Tracking System (FTS) is SBA's web-based database for tracking FOIA and PA requests and appeals. It establishes a record of a request that includes requester details, dates of correspondence between SBA and the requester, the subject of the request, the actions taken by SBA until the final disposition, and what office is assigned to undertake each action. It also produces reports based on queries by office, subject, dates, etc.

Use of the FTS is mandatory; designated Contacts or their Back-ups must enter data into the FTS within 48 hours of receipt of a FOI/PA inquiry. Pertinent status and tracking data must be entered once an office has taken action.

Only the Contacts and Back-ups have access to the FTS through designated User IDs and Passwords.

Only the FOI/PA Office can view and access all data in the FTS. All other SBA offices can only view and access data on cases they have entered or that have been assigned to them.