

## DOCUMENT RESUME

06216 - [ E1586617 ]

Agencies' Implementation of and Compliance with the Privacy Act Can Be Improved. LCD-78-115; B-130441. June 6, 1978. 27 pp. + appendix (2 pp.).

Report to James T. McIntyre, Jr., Director, Office of Management and Budget; by Victor L. Lowe, Director, General Government Div.

Issue Area: Federal Information: Implementing the Privacy Act of 1974 (1401).

Contact: Logistics and Communications Div.

Budget Function: General Government: General Property and Records Management (804).

Organization Concerned: Department of Agriculture; Department of the Navy; Department of the Army; Department of Commerce; Department of the Air Force; Department of Health, Education, and Welfare; Department of Justice; Department of Labor; Department of State; Department of Transportation; Department of the Treasury; Veterans Administration.

Authority: Privacy Act of 1974 (P.L. 93-579). Freedom of Information Act. CMB Circular A-108.

The Privacy Act of 1974 provides certain safeguards to individuals against invasion of privacy by requiring Federal agencies to establish rules and procedures for maintaining and protecting personal data in agency record systems. As of December 31, 1976, Federal agencies had 6,753 systems of records which contained 3.85 billion records about individuals, and operating costs relevant to the act for the year ended September 30, 1976, were an estimated \$36.6 million.

Findings/Conclusions: Agencies are making a concerted effort to implement and comply with provisions of the act, but improvements are needed. Three systems of records had not been published in the Federal Register, but action is being taken to comply with this requirement. In several instances, forms used for collecting information from individuals did not contain required notices about information disclosure. According to officials, a policy of providing access to information was followed, and data identifying confidential sources of information were deleted. Agencies must keep an accurate accounting of statistics for certain disclosures, and the accounting must be available to the subject upon request. The estimated cost for agencies to account for disclosures for the year ended September 30, 1976, was \$9.4 million. The adequacy of disclosure accounting could not be readily determined because of the methods used. Reductions in paperwork and staff time might be achieved by eliminating duplication and changing certain accounting procedures. Employees were receiving Privacy Act training, but the adequacy of training was not fully evaluated. Recommendations: The Office of Management and Budget should encourage heads of departments and agencies to review periodically the manner in which requirements of the act are

being fulfilled to determine needs for additional training or other action; emphasize the opportunities for reducing the cost of accounting for disclosures, with a view toward eliminating duplication and paperwork; determine whether agencies should be required to maintain accountings for disclosures from locator files where individuals have authorized release of such information; and advise agencies to make greater use of one-time Privacy Act notices or revise forms to incorporate notices.

(HTH)

6617

---

REPORT BY THE U.S.

# General Accounting Office

---

## Agencies' Implementation Of And Compliance With The Privacy Act Can Be Improved

Federal agencies are making a concerted effort to implement and comply with the Privacy Act. Various instances of noncompliance were identified at the locations reviewed. The noncompliance appeared to result from misinterpretation of the act or guidelines or unfamiliarity with the act.

Periodic evaluations of Privacy Act compliance should be made at agency locations to determine whether additional training or other action is required. Also, opportunity exists for reducing paperwork and administrative workload.



LCD-78-115  
JUNE 6, 1978



UNITED STATES GENERAL ACCOUNTING OFFICE  
WASHINGTON, D.C. 20548

GENERAL GOVERNMENT  
DIVISION

B-130441

The Honorable James T. McIntyre, Jr.  
Director, Office of Management and Budget

Dear Mr. McIntyre:

This is our report on how agencies' implementation of and compliance with the Privacy Act can be improved.

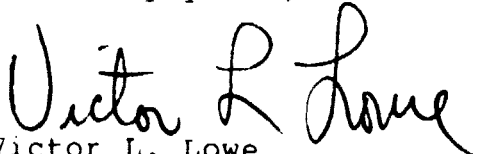
Agencies are making a concerted effort to implement and comply with the act, but various instances of noncompliance were identified at locations visited. Periodic evaluations of Privacy Act compliance could improve the manner in which the provisions of the act are being carried out. In addition, opportunity exists for reducing paperwork and administrative workload related to the act.

As you know, section 236 of the Legislative Reorganization Act of 1970 requires the head of a Federal agency to submit a written statement on actions taken on our recommendations to the House Committee on Government Operations and Senate Committee on Governmental Affairs not later than 60 days after the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of the report.

Copies of the report are being sent to the House Committee on Government Operations, the Senate Committee on Governmental Affairs, and the House and Senate Committees on Appropriations. Copies of the report are also being sent to interested congressional committees and subcommittees and to Federal departments and agencies.

If you wish, we will be pleased to discuss the details of the report with you or your staff.

Sincerely yours,

  
Victor L. Lowe  
Director

D I G E S T

This study of agencies' experiences in implementing and complying with the Privacy Act of 1974 was undertaken because of the considerable congressional and public interest in privacy and the newness of the act. GAO's purpose was to study in limited depth how the numerous provisions of the Privacy Act were being carried out and to identify specific areas requiring in-depth study. However, because of the interest in privacy and the study's identification of certain areas needing improvement, GAO is providing the results of the study to various congressional committees and subcommittees, the Office of Management and Budget, and Federal departments and agencies.

The purpose of the Privacy Act of 1974 is to provide certain safeguards to individuals against invasion of personal privacy by requiring Federal agencies to establish rules and procedures for maintaining and protecting personal data in agency record systems. The act became effective on September 27, 1975.

As of December 31, 1976, Federal agencies had 6,753 systems of records which contained 3.85 billion records about individuals. Operating costs relevant to the Privacy Act for the year ended September 30, 1976, were an estimated \$36.6 million.

FINDINGS

In our opinion, agencies are making a concerted effort to implement and comply with the provisions of the Privacy Act. However, improvements can be made in how the provisions of the act are being implemented and carried out.

GAO's review was performed at 28 locations representing 11 civil agencies (20 locations) and at 8 Department of Defense locations. (See p. 28.) At the locations visited, GAO found three systems of records that had not

been published in the Federal Register as required by the act, but action was being taken to comply with the act. (See p. 7.)

Agencies, when collecting information from individuals, are required to advise them in writing of why the information is needed, whether it is voluntary or mandatory, and what the consequences are if the information is not provided. GAO found several instances where forms used for collecting information did not contain this notice or related information. For example, the Agriculture Stabilization and Conservation Service, Sangamon County, Illinois, solicited information from farmers concerning price support payments, but a Privacy Act notice was not provided. (See p. 8.)

Representatives at the locations visited had mixed feelings as to whether the Privacy Act has impeded the collection of information from individuals. However, assuring confidentiality to third-party sources was cited as a potential problem at numerous agencies. (See p. 12.)

Officials at the locations visited professed a policy of providing requestors with access to information in their files and as much information as possible. The Department of Defense, for example, encouraged employees to examine their files even before passage of the Privacy Act. In addition, St. Elizabeths Hospital informs patients, upon admission to the hospital, of their right to examine their records. Locations maintaining information obtained confidentially generally provided information to requestors, but deleted data that would identify the source. (See p. 13.)

Accounting for disclosures has probably had the greatest impact on agencies maintaining large volumes of personal information. The act requires that for certain disclosures of individuals' records, agencies must keep an accurate accounting of the date, nature, and purpose of each disclosure to any person or agency, and the name and address of the person or agency to whom the disclosure is made. This accounting must be made available to the subject at his or her request. In addition, corrected or disputed

records must be provided to prior recipients of such records. (See p. 15.)

The estimated cost for Federal agencies to account for disclosures for the year ended September 30, 1976, was \$9.4 million, or 26 percent of the operating costs applicable to the Privacy Act. Although most locations visited had established an accounting of disclosures, the accuracy and adequacy of the accountings could not readily be determined in all instances because of the methods used in accounting for disclosures. For example, Office of Guaranteed Student Loans officials reported that they make about 35 million routine disclosures annually but do not have the computer capability to account for each routine disclosure of every record in the system. The officials estimate that an investment of \$50-80 million would be needed to develop a computer system for this purpose. GAO was told that currently, a "reconstruction" procedure is used wherein they can determine the approximate time-frame of a disclosure and to whom the disclosure was made. However, based on discussions with various agency officials, GAO is not confident that the disclosure accounting problem has been resolved. (See pp. 15 and 16.)

There appears to be a potential for reducing paperwork costs and staff time by eliminating duplication and in accounting for records requiring automatic disclosure (normal distribution to other agencies required by other laws or directives). (See p. 17.) In addition, the need to account for certain other types of disclosures, such as ones from locator files, seems unnecessary. (See p. 19.)

Locations visited had provided some type of Privacy Act training for employees whose duties were directly affected by the law. While GAO found various instances of noncompliance with the act, no in-depth evaluation was made to determine whether this was due to inadequate training or inadequate implementation of procedures presented during training sessions. (See p. 21.)

Benefits cited as resulting from the Privacy Act were (1) the opportunity for individuals

to have access to and amend their records, (2) greater awareness of the need for protecting personal data, (3) the destruction of unnecessary systems of records, (4) the requirement to advise individuals asked to furnish information whether it is mandatory or voluntary to provide the data and the consequences of not furnishing the data, and (5) the intangible benefit of promoting public goodwill. Problems cited as resulting from the act were (1) the additional paperwork, workload, and cost of accounting for disclosures; (2) the potential for restricting exchange of information; (3) the problem of protecting the confidentiality of third parties; and (4) the potential problem of pretrial discovery. (See p. 23.)

### CONCLUSIONS

GAO believes that agencies are making a concerted effort to implement and comply with the Privacy Act, but improvements can be made. Because of the various instances of noncompliance found at agency locations, GAO believes there is a need for periodically evaluating the manner in which agency locations are carrying out the provisions of the act to determine if additional training or other action is required.

GAO believes also that considerable opportunity exists for reducing administrative workload, paperwork, and related costs.

### RECOMMENDATIONS TO THE OFFICE OF MANAGEMENT AND BUDGET

To insure that agency locations are complying with the Privacy Act, and to reduce the cost of carrying out the provisions of the act, we recommend that the Office of Management and Budget:

- Encourage heads of departments and agencies to periodically review the manner in which installations are fulfilling the requirements of the Privacy Act to determine whether additional training or other action is necessary.
- Emphasize to agencies the opportunities for reducing the cost of accounting for



disclosures by evaluating their methods of maintaining the accountings, with a view toward eliminating duplication and unnecessary paperwork.

- Determine whether agencies should be required to maintain accountings for disclosures from locator files where individuals have authorized release of such information.
- Advise agencies to make greater use of one-time Privacy Act notices, where practicable, or revise forms to incorporate the notices.

Office of Management and Budget officials generally agreed with the recommendations and advised us that actions would be taken in accordance with the recommendations.

# C o n t e n t s

		<u>Page</u>
DIGEST		i
CHAPTER		
1	INTRODUCTION	1
	What is the Privacy Act?	1
	What the Privacy Act requires of Federal agencies	2
	How many personal systems of records in Federal agencies?	4
	The costs of implementing the Privacy Act	5
2	AGENCIES' IMPLEMENTATION OF AND COMPLIANCE WITH THE PRIVACY ACT CAN BE IMPROVED	7
	Systems of records not published in Federal Register	7
	Privacy Act notices not always provided	8
	Various actions by agencies to eliminate unneeded data	10
	Effect of Privacy Act on data collection	12
	Protection of manual records appears adequate	13
	Individuals requesting data appear to receive access to files	13
	Small number of requests for amendment of records	14
	Need for improvements in accounting for disclosures	15
	Opportunities for reducing cost of accounting for automatic disclosures	17
	Questionable value of accounting for certain types of disclosures	19
	Copy fees vary among agencies	20
	Need to periodically evaluate effectiveness of staff training	21
3	LOCATIONS CITE BENEFITS AND PROBLEMS OF THE PRIVACY ACT	23
	Benefits	23
	Problems	24

CHAPTER

4	CONCLUSIONS AND RECOMMENDATIONS	25
	Conclusions	25
	Recommendations	25
5	SCOPE OF REVIEW	27

APPENDIX

I	Installations and locations included in this review	28
---	--	----

ABBREVIATIONS

DEA	Drug Enforcement Administration
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
OMB	Office of Management and Budget
VA	Veterans Administration

## CHAPTER 1

### INTRODUCTION

This study of agencies' experiences in implementing and complying with the Privacy Act of 1974 was undertaken because of the considerable congressional and public interest in privacy and the newness of the act. Our purpose was to study in limited depth how the numerous provisions of the Privacy Act were being carried out and to identify specific areas requiring comprehensive coverage. The results of the study were intended for internal use in planning in-depth studies. However, because of the interest in privacy and the study's identification of certain areas needing improvement, we are providing the results of the study to various congressional committees and subcommittees, the Office of Management and Budget (OMB), and Federal departments and agencies.

Early in the study we recognized several areas which appeared to require in-depth review, and studies are underway in these areas. The studies cover (1) the protection of personal data in automated systems, (2) the effect of Privacy Act limitations on the exchange of information between Federal agencies, and (3) the experiences of individuals requesting personal information from Federal agencies.

#### WHAT IS THE PRIVACY ACT?

The purpose of the Privacy Act of 1974 (Public Law 93-579, Dec. 31, 1974) is to provide certain safeguards to individuals against invasion of personal privacy by requiring Federal agencies to establish rules and procedures for maintaining and protecting personal data in agency record systems. The act became effective on September 27, 1975.

The act gives an individual (1) the right to know what records pertaining to him or her are collected, maintained, used, or disseminated by the agencies; (2) the right to have access to agencies' information pertaining to him or her (with certain exceptions) and to amend or correct the information; and (3) the right to prevent information obtained by agencies for a specific purpose from being disclosed for another purpose without his or her consent.

The act also requires an agency to insure that any record of identifiable personal information maintained by an agency is for a necessary and lawful purpose, that it is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information. Agencies are subject to civil suit, and Government

employees are subject to a penalty of up to \$5,000 for any damages which occur as a result of willful or intentional criminal action violating any individual's rights under the act.

The Privacy Act complements earlier legislation--the Freedom of Information Act--which makes information maintained by Federal agencies available to the public subject to certain exemptions, such as when its release represents a clearly unwarranted invasion of personal privacy.

#### WHAT THE PRIVACY ACT REQUIRES OF FEDERAL AGENCIES

A basic premise of the law is that information about individuals should not be maintained in secret files. Agencies are required to publish at least annually in the Federal Register various data relevant to all of their systems of records containing information about individuals. A system of records is defined as a group of any records under the control of any agency from which information is retrieved by an individual's name, or some identifying number, symbol, or other identifying particular assigned to the individual. Information to be published in the Federal Register includes a description of the categories of records maintained, the types of sources for the information, and the routine uses of the records.

Upon request, an agency must permit the subject of a record to gain access to and copy his or her record. An individual disagreeing with the contents of the record may request an amendment to it. If the request is denied, or not satisfactorily resolved, an individual may appeal the decision within the agency. Then, if the matter is still unresolved, the individual may appeal the matter to a district court and/or place a statement about the disagreement in the record. The agency is required to distribute the statement of disagreement with all subsequent disclosures of the record, and to any person or agency to whom disclosures of the record have previously been made.

Records contained in a system of records may not be disclosed by an agency without the consent of the subject of the record, unless the disclosure is specifically permitted by the act. There are 11 categories of permissible disclosures, including, among others, disclosures to employees of the agency that maintains the record who have a need for the record in the performance of their duties; disclosures required under the Freedom of Information Act; disclosures to the Congress, the courts, and GAO; and

disclosures for a routine use. Routine use, with respect to disclosures, is defined in the act as the use of a record for a purpose compatible with the purpose for which the record was collected. The routine uses must be included in the published descriptions of systems in the Federal Register.

The act permits systems of records maintained by the Central Intelligence Agency or agencies involved in law enforcement to be exempted from many of the act's provisions. More limited exemptions are permitted for systems of records that contain classified information, statistical data, or information from confidential sources. The exemption provisions, however, are permissive and not mandatory; they apply to a system of records only when specifically invoked by the head of an agency.

Except for disclosures to agency employees in the performance of their duties and disclosures required under the Freedom of Information Act, agencies are also required to keep an accounting of the dates, nature, and purpose of disclosures, as well as the names and addresses of the persons or agencies to whom the records were disclosed. Prior recipients of data must be notified of all subsequent corrections to the record and any disputes about the contents.

Other provisions of the act require that agencies

- maintain only information that is relevant and necessary to accomplish a legal purpose of the agency;
- collect information to the greatest extent practicable directly from the subject when the use of the information may result in an adverse determination;
- inform each individual asked to supply personal information of the authority for the request, the principal purpose for which the information will be used, any routine uses, the consequences of failing to provide the requested information, and whether the disclosure is mandatory or voluntary;
- maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness when disseminating information to others;
- maintain no records describing how any individual exercises rights guaranteed by the First Amendment (religion, beliefs, or association) unless

- expressly authorized by statute or unless the records are pertinent to authorized law enforcement activities;
- establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records;
  - sell or rent mailing lists only when specifically authorized by law; and
  - promulgate rules to implement these provisions.

The act also makes it unlawful for any Federal, State, or local government agency to deny an individual any right, benefit, or privilege provided by law because an individual refuses to disclose his or her social security number, unless (1) the disclosure is required by Federal statute or (2) a system of records was in existence before January 1, 1975, and the disclosure was required under statute or regulation to verify the identity of an individual. Any of the agencies that request an individual to disclose his or her social security number must inform the individual of whether the disclosure is mandatory or voluntary, what the applicable statute or other authority is, and what uses will be made of the social security number.

OMB was given responsibility for developing guidelines and regulations for agencies to use in implementing the provisions of the act. OMB issued Circular No. A-108--Responsibilities for the Maintenance of Records About Individuals by Federal Agencies--and Privacy Act implementation guidelines in July 1975. The Office also issued supplementary guidance to agencies in November 1975, and issued four supplements to Circular No. A-108 at various times between 1975 and 1978.

#### HOW MANY PERSONAL SYSTEMS OF RECORDS IN FEDERAL AGENCIES?

The Second Annual Report of the President, "Federal Personal Data Systems Subject to the Privacy Act of 1974," showed that as of December 31, 1976, 97 agencies maintained 6,753 personal systems of records containing 3.85 billion individual records, a net increase of 11 agencies and 30 systems, and a net decrease of 34 million individual records from 1975. Fifty-seven percent (3,822) of the systems are maintained by three agencies--the Department of Defense (2,219); the Department of the Treasury (910); and the Department of Health, Education, and Welfare (693).

The report showed that 4,566 of the 6,753 systems, or 68 percent, are for in-house agency administrative purposes. Most of the individual records--3.2 billion of the 3.85 billion records, or 83 percent--are in the remaining 2,187 systems which deal with the operation of various Federal programs. About 60 percent of the 3.2 billion individual records maintained for program purposes are contained in only 12 systems--6 Treasury Department systems (721 million records); 4 Social Security Administration systems (740 million records); and 2 Department of Commerce census systems (406 million records).

#### THE COSTS OF IMPLEMENTING THE PRIVACY ACT

On the basis of cost data that OMB received from 85 executive branch agencies which had published rules and notices of records subject to the act, start-up or one-time costs for implementing the Privacy Act were estimated at \$29.5 million during the period January 1, 1975, to September 30, 1976. Operating costs relevant to the act for the period September 27, 1975, through September 30, 1976, were estimated at \$36.6 million.

OMB in a March 1977 report pointed out that the cost data, for the most part, represents only agencies' educated estimates, because collecting useful cost data is difficult. The imprecision occurs because the act affects virtually every organization in every agency, and it is often not possible to sort out costs attributable to the act. Furthermore, in many instances the act does not establish a new program or activity, but rather affects the way agencies perform existing functions.

Costs related to various provisions of the act are shown in the following schedule prepared by OMB.



<u>Item</u>	<u>Start-up costs</u>		<u>Operating costs</u>	
	<u>Amount</u>	<u>Percent</u>	<u>Amount</u>	<u>Percent</u>
	(thousands)		(thousands)	
Publication requirements	\$13,549	46.0	\$ 4,405	12.0
Training	6,825	23.2	3,282	9.0
Granting access	914	3.1	10,670	29.2
Correcting records	483	1.6	2,116	5.8
Security and control	2,175	7.4	1,345	3.7
Accounting for disclosures	667	2.3	9,415	25.7
New data collection procedures	1,164	4.0	1,507	4.1
Other	3,728	12.7	4,012	11.0
Reductions from records/systems eliminated	-45	-0.2	-62	-0.2
Collections	<u>-2</u>	<u>-</u>	<u>-91</u>	<u>-0.2</u>
Total (net) (note a)	<u>\$29,459</u>	<u>100.0</u>	<u>\$36,559</u>	<u>100.0</u>

a/Totals do not add due to rounding.

As shown in the schedule, publication requirements and training costs were \$20.4 million, or 69 percent of the start-up costs. The major operating costs were attributable to granting access to records and accounting for disclosures; these costs totaled \$20.1 million, or 55 percent of the operating costs.

The report showed that most of the start-up and operating costs were borne by 21 major recordkeeping agencies--\$27.2 million (92 percent) of the total start-up costs, and \$35.5 million (97 percent, of the total operating costs. The OMB report defined major recordkeeping agencies as those with 45 or more systems.

## CHAPTER 2

### AGENCIES' IMPLEMENTATION OF AND

### COMPLIANCE WITH THE PRIVACY ACT

#### CAN BE IMPROVED

In our opinion, agencies are making a concerted effort to implement and comply with the provisions of the Privacy Act. At the time of our review, agencies had about 1 year's experience working under the act. Because of the newness of the act, there have been varying interpretations by agencies of the provisions of the act and how the provisions should be carried out. Some locations are more advanced than others in both their familiarity with the act and the methods used in complying with the act's provisions. It seemed apparent, however, that locations away from headquarters offices were generally less knowledgeable about the act and its requirements, even though implementing regulations and directives had been provided to field locations. This occurred in some instances because of the limited Privacy Act activity at the field locations. We found various instances of noncompliance with the act which appeared to result from misinterpretation of the act or guidelines or from unfamiliarity with the act, rather than deliberate agency action to avoid the intent of the act.

The following sections discuss actions taken at the locations reviewed to implement and comply with the act. Locations cited as examples in the report were selected for the purpose of illustration only. Such selection is not meant to infer either approval or criticism of all Privacy Act activities at these locations.

#### SYSTEMS OF RECORDS NOT PUBLISHED IN FEDERAL REGISTER

A basic premise of the Privacy Act is that information about individuals should not be maintained in secret files. The act requires each agency maintaining a system of records on individuals to publish annually in the Federal Register a notice of the existence and character of records systems. At the locations visited, we became aware of three systems of records that had not been published in the Federal Register. It should be emphasized, however, that systems of records purposely kept secret could go undetected.

We were told of two systems of records not published in the Federal Register, which were stored at the National

Personnel Records Center, Civilian Personnel Records, in St. Louis. The records center functions as a repository only. One system of records was World War II investigative files of the Office for Emergency Management; the second system was Post Office Inspection Service files covering the period 1936-47. The records center was attempting to locate someone with the authority to determine if the files could be destroyed. The third system of records is the Civil Service Commission's Investigator Performance Files, which pertain primarily to investigators' performance. Through oversight this system of records was not published in the Federal Register. However, Commission officials advised us that a notice is being prepared for publication in the Federal Register.

PRIVACY ACT NOTICES  
NOT ALWAYS PROVIDED

The Privacy Act requires that, if information is collected from individuals, these persons should be given notice in writing of:

- The authority to solicit the information (whether it is granted by statute or by Executive Order of the President).
- Whether the information to be provided is mandatory or voluntary.
- What the information is to be used for.
- The routine uses of the information.
- What the consequences will be if all or part of the information is not provided.

Our examination of Privacy Act notices used when collecting information showed that, generally, locations reviewed were complying with the requirements. However, we did find several instances where forms used for collecting information did not contain a Privacy Act notice or related information.

Three of 11 forms used by the St. Louis District U.S. Army Corps of Engineers did not include the authority and routine uses of the data. Another District questionnaire used to collect relocation information had no Privacy Act notice. The Agriculture Stabilization and Conservation Service, Sangamon County, Illinois, solicited information from farmers concerning price support payments, but a Privacy Act notice was not provided.

Another exception was Lowry Air Force Base, Denver, Colorado, which was not providing Privacy Act notices to prisoners when taking fingerprints and photographs for the Correction Records System. Some individuals responsible for collecting information felt that the correction records were automatically exempt from the Privacy Act notice requirement because they were law enforcement records. Since a notice announcing that the records were exempt had not been published in the Federal Register, as required by subsections (j) or (k) of the act, Privacy Act notices should have been provided to the prisoners. After we pointed out that the Correction Records System had not been exempt, Lowry instituted a procedure to provide Privacy Act notices when collecting fingerprints and photographs.

We noted also that Privacy Act notices involving travel claims differed at various agencies, and, in some instances, were causing increased paperwork. Travel vouchers generally contain such personal information as travel itineraries and motel receipts. The Securities and Exchange Commission requires a notice, signed by the individual, to be attached to each travel voucher no matter how many vouchers are submitted by the same individual. The Fitzsimons Army Medical Center, Denver, had a similar procedure.

Lowry Air Force Base simply posts a notice in a conspicuous place in the travel office. The poster informs individuals that they may have a copy if they want it. Lowry does not require a notice for each travel voucher. The Veterans Administration Denver Regional Office distributes a one-time notice to each employee. The Office does not attach a copy to each voucher.

The Department of Labor had no procedure for providing notices to employees. An official at the Department of Labor Denver Regional Office, after our discussion, called his Washington, D.C., office and was informed that the Department had no procedures on this subject. The Washington office directed the Denver official to prepare a procedure for the entire Department.

Securities and Exchange Commission representatives contend that an initial notice with the first voucher should be adequate, but said that the General Services Administration requires them to have a notice with each travel voucher.

The General Services Administration advised us that Standard Form 1012 (Travel Voucher) was revised to incorporate a Privacy Act notice and became available in May 1978.

It appears to us that a one-time notice would meet the requirement of the act when the same forms, such as travel vouchers, are completed several times by the same person.

VARIOUS ACTIONS BY AGENCIES  
TO ELIMINATE UNNEEDED DATA

OMB guidelines provide that agencies, at least annually, should assess the legality of, need for, and relevance of information contained in each of their systems of records. Agencies, however, are not required to examine the actual contents of records, but must consider the relevance of, and necessity for, the general categories of information maintained.

To varying degrees, agencies were looking at information in their systems of records to determine if information could be eliminated, as well as reviewing the need for information being collected. Invoking this review procedure led to instances where record systems had been eliminated, information unrelated to the file's purpose was being removed, and forms were discontinued or revised to eliminate unneeded data.

For example, the Army Reserve Components Personnel and Administration Center eliminated a listing of Adjutant General Corps colonels, and the St. Louis District U.S. Army Corps of Engineers eliminated a file of employees holding Government driver's licenses. The Securities and Exchange Commission also eliminated a system of records--Organized Crime Index Cards--that had been maintained prior to the act; the Engineer District Office removed race designations from personnel files; the General Services Administration required personnel files to be purged of various data; the Army Aviation Systems Command, St. Louis, is purging unneeded data from personnel files as time permits; and other locations visited were revising or eliminating forms, including the Fitzsimons Army Medical Center, Denver, which revised or eliminated 80 of 425 local forms.

We did note some instances, however, where more information was being collected and maintained than appeared necessary. For example, one type of record which is necessary for an initial determination by the Veterans Administration's Philadelphia Center, but which is not necessary to be retained as a part of a record system or as a record system itself, is copies of investigative reports obtained from the Federal Bureau of Investigation (FBI). We were advised by Veterans Administration (VA) officials that they retain FBI investigative reports for about 2 years.

As of December 1976, reports were maintained by VA's Philadelphia Center on 37 individuals and 28 schools. A VA official told us that only the results of the investigations are necessary, and he felt that the Administration did not have to retain the reports.

It should be noted that these reports are duplicate reports. The originals are retained by the FBI and are considered by VA to be an FBI record system. Since only the results of the investigation are necessary and the original reports are available at the FBI, the retention of these investigative reports by VA is questionable.

A similar situation has occurred with military court martial files. VA insurance may be canceled as a result of certain court martial findings. VA receives complete copies of court martial files, although only the decision is necessary, and the court martial files become a part of individuals' insurance files. Since the Privacy Act requires an agency to insure that any record of identifiable personal information maintained by an agency is for a necessary and lawful purpose, it seems that the practice of maintaining unnecessary court martial files should be discontinued.

Records at some locations contained information relating to First Amendment rights (religion preference and association or affiliation data). The Civil Service Commission, for example, collected information on employment applicants' beliefs, activities, and groups and persons associated with the individuals. We were told that such information on individuals is no longer collected by the Commission. The Commission obtained funds for additional staff positions for the purpose of removing this data from existing files. Records at various military locations sometimes include religious preference. The military retains this information to notify the proper clergyman should a serviceman be seriously injured or die while on duty.

Various actions are being taken by agencies to review the need for information collected and to purge unneeded data from files. Considerable effort would be required to eliminate all unneeded data from all files, especially the more voluminous systems of records. Until this occurs, however, agency files will continue to contain information that may no longer be relevant or necessary.

EFFECT OF PRIVACY ACT  
ON DATA COLLECTION

Representatives at the locations visited had mixed feelings as to whether the Privacy Act impedes the collection of information from individuals. However, assuring confidentiality to third-party sources was cited by numerous agencies as a potential problem in collecting information, since the courts could ultimately determine that the information should be released.

Customs Service officials stated that they have always dealt with confidential information and said the Privacy Act has not changed their policy to a great extent. However, they feel that informants may become reluctant to provide information. A VA official also said that third parties are becoming reluctant to cooperate with Federal agencies, because the information may subsequently be released.

Agencies involved in police and investigative work frequently take information confidentially from third-party sources. If a source's name was later retrieved by a subject, it could jeopardize the safety of the third party or at least limit that person's usefulness. According to one official, the fear that knowledge provided in confidence will later be revealed deters third parties from offering information and impairs investigative efforts. These views were expressed at the Drug Enforcement Administration (DEA), the FBI, the Department of State, and the Civil Service Commission.

The Civil Service Commission's San Francisco Regional Office surveyed third-party responses to inquiries sent out as part of full field background investigations of candidates for Federal employment. One group of inquiries was sent out before the effective date of the Privacy Act, and a second group was sent out after the act became effective. The Regional Office found a 24.8-percent decrease in the rate of derogatory written responses, from 4.9 percent of the pre-act group to 3.7 percent of the post-act group. The survey stated that the difference apparently resulted from the post-act addition of a Privacy Act statement, that is, an explanation of the subject's entitlement to see the information that is furnished. The survey pointed out that this was only a sample survey of one office, but it was felt that similar findings would occur in other offices.

DEA reported an unquantifiable decrease in the inter- and intra-agency flow of information apparently prompted by

a fear of violating the law, or else a fear of losing confidentiality. DEA officials said confidentiality can be pledged to a third party, but cannot be guaranteed because the courts have the final jurisdiction in cases of appeal.

PROTECTION OF MANUAL RECORDS  
APPEAR ADEQUATE

The physical protection of manual records at most locations visited appeared adequate. Records were either filed in locked cabinets, locked rooms, or in controlled areas restricted to authorized personnel. Records at the Air Reserve Personnel Center, for example, are maintained in a controlled area and access to the area is limited to authorized personnel. The area is locked after closing hours. Similar protection was found at most of the other locations.

We did not determine the reasonableness of computer data security for personal information due to the considerable time necessary to evaluate the various complexities of computer security; this subject will be covered in a separate review.

INDIVIDUALS REQUESTING DATA APPEAR  
TO RECEIVE ACCESS TO FILES

The Privacy Act requires agencies to allow an individual, upon request, to gain access to information about him or her contained in a system of records, subject to certain exemptions such as investigative data or data that would reveal the identity of a confidential source.

Locations visited professed a policy of providing requestors with access to information in their files and as much information as possible. The Department of Defense, for example, encouraged employees to examine their files even before passage of the Privacy Act. In addition, St. Elizabeths Hospital informs patients, upon admission to the hospital, of their right to examine their records. Agencies maintaining information obtained confidentially usually provided information to requestors, but deleted data that would identify the source.

Agencies such as the FBI, DEA, the Department of State, and the Department of Agriculture's Office of Investigations, that have systems of records exempted from provisions of the Privacy Act, said they take into consideration the release provisions of the Freedom of Information Act as well as the Privacy Act, and will release as much data as possible from these systems. For example, the FBI will provide individuals with access to their records as



long as the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal, civil, or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants, and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede law enforcement.

We were told by officials at various locations that almost all requests for information by individuals are general in nature. An individual usually requests all information in the agency's files concerning him or her. Individuals generally do not cite a specific system of records published in the Federal Register, nor do they cite the Privacy Act or the Freedom of Information Act. Regarding the publication of systems of records in the Federal Register, it does not appear that this is the proper vehicle for providing assistance to the general public for requesting data from agencies. It does, however, serve the purpose of requiring agency accountability for personal systems of records and provides a basis for congressional oversight.

In responding to inquiries, locations with numerous record systems generally search only their major systems, unless the requestor identifies a specific system of records. For example, when DEA receives a request, it checks its two major systems to see if they contain information on the requestor. According to one DEA official, these checks provide "97 to 98 percent accuracy" as to whether DEA has any information on the requestor. We were advised, however, that if an individual identifies himself as a doctor, lawyer, pilot, etc., checks of any system of records that would apply to the particular occupation would also be made. Once the information is compiled and information not to be released has been deleted, it is forwarded to the requestor. If the search for information regarding the requestor is negative, the requestor is so notified.

#### SMALL NUMBER OF REQUESTS FOR AMENDMENT OF RECORDS

The Privacy Act requires each agency maintaining a system of records to permit the subject to request amendment of a record. with the exception of one location, most locations visited had a small number of requests for correction or amendment of records.

According to records at the Army Reserve Components and Personnel Administration Center, between September 27,

1975, and December 31, 1976, the Center received 22,000 requests from reservists to amend their military personnel files. Fewer numbers of requests to amend records were received by other locations such as the FBI, which had received 150 requests for amendment of records as of October 17, 1977.

Officials at three locations--Philadelphia Naval Regional Medical Center; General Services Administration's Area Personnel Office, St. Louis; and the Army Aviation Systems Command, St. Louis--advised us that they had received no requests for amendments to records in the systems covered in our review.

#### NEED FOR IMPROVEMENTS IN ACCOUNTING FOR DISCLOSURES

Probably the greatest impact on agencies maintaining large volumes of personal information has been the accounting for disclosures. The act requires that agencies keep an accurate accounting of the date, nature, and purpose of each disclosure to any person or agency, and the name and address of the person or agency to whom the disclosure is made. This accounting must be made available to the subject at his or her request. If any corrections or disputes are involved with the information, prior recipients of the data must be informed of the correction or the dispute. The act requires that agencies retain the accounting for at least 5 years or the life of the record, whichever is longer.

According to OMB, the estimated cost of accounting for disclosures by Federal agencies during the year ended September 30, 1976, was \$9.4 million, or 26 percent of the total operating costs applicable to the Privacy Act.

Although installations visited have established an accounting for disclosures, the accuracy and adequacy of the accountings cannot readily be determined in all instances because of the methods used in accounting for disclosures. In addition, duplicate systems of records being maintained by some locations result in increased paperwork and additional cost.

The Privacy Act prohibits the disclosure of a record, by any means, without the consent of the individual. However, the act establishes 11 exceptions to this rule. Disclosures can be made (1) to agency personnel that have a need for the record in the performance of their duties; (2) as required under the Freedom of Information Act; (3) for "routine uses" as published in the Federal Register;

(4) to the Bureau of the Census; (5) for statistical research; (6) to the National Archives; (7) upon written request, to a civil or criminal law enforcement activity authorized by law; (8) for the health and safety of an individual; (9) to either House of Congress or subdivisions; (10) to the Comptroller General or his representatives during the performance of duties of the General Accounting Office; and (11) pursuant to a court order. With the exception of the first two items, each agency must keep an accurate accounting of disclosures.

Neither the act's nor OMB's implementing guidelines specify a method of accounting for disclosures. OMB guidelines provide that an agency may use any system it desires for keeping notations of disclosures, provided that it can construct from its system a document listing all disclosures.

Ways of meeting this requirement vary from agency to agency. These range from agencywide centralized automated systems to notation of the distribution on the record disclosed. Generally, the more records in the system, the more sophisticated the accounting system.

Following are some of the methods used by installations to account for disclosures.

- Officials of the Office of Guaranteed Student Loans, Department of Health, Education, and Welfare, reported that with a file of about 8.5 to 10 million records, from which 35 million routine disclosures are made annually, they do not have the computer capability to account for each routine disclosure of every record in the system. They estimate an investment of \$50-\$80 million would be needed to develop a computer system for this purpose. An attempt to eliminate the accounting of disclosure requirement by having loan applicants consent to waiving such accountings was discarded after a lawsuit was filed by several applicants and later dismissed by stipulation. We were advised that currently, a "reconstruction" procedure is used to account for disclosures wherein they can determine the approximate timeframe of a disclosure and who the disclosure was made to. However, based on discussions with various agency officials, we are not confident that the disclosure accounting problem has been resolved.
- DEA maintains a centralized automated disclosure accounting system which provides information on disclosures to individuals, as well as routine use

disclosures to law enforcement activities outside of the Department of Justice. A hard copy disclosure accounting record is also maintained by the field office making the disclosure.

- The Army Reserve Components Personnel and Administration Center in St. Louis places a disclosure accounting form in the subject's file, but does not maintain a separate log of all disclosures. This system easily identifies disclosures from the files.
- Customs Service officials in the Baltimore Region said that a Privacy Act disclosure record form is maintained for most disclosures. A copy of the form is inserted into the individual's file and a master file, and one is sent to headquarters.

The method of accounting for disclosures also varies within the same agency. For example, disclosures of information from the Philadelphia VA Center's Government life insurance record system are accounted for by making an entry in a disclosure log and filing a copy of the written replies to requesting parties in a centralized file. Within the Center, another division keeps an accounting for another system of records by preparing a disclosure form. The original form is placed in the individual's file, and a carbon copy is kept separate for easy reference.

Social Security Administration officials also have different methods of accounting for disclosures. One official said that a copy of a response to a request is placed in the individual's file or coded on the automated record system. Another official said the record of disclosure is noted on the automated record system for all disclosures, but an accounting is not kept in the individual's file.

At those installations that have received a small number of requests for data, disclosure accounting has been fairly easy and a manual filing system has been sufficient to keep an accounting in most cases. However, in organizations experiencing a heavy disclosure workload, such as the Office of Guaranteed Student Loans and DEA, disclosure accounting becomes much more burdensome.

#### OPPORTUNITIES FOR REDUCING COST OF ACCOUNTING FOR AUTOMATIC DISCLOSURES

There appears to be a potential for reducing paperwork costs and staff time in accounting for records requiring

automatic disclosure (normal distribution to other agencies required by other laws or directives). As stated in OMB's guidelines, an agency may use any system to keep notations of disclosures, provided it can construct from its system a document listing all disclosures. This indicates that it is not necessary to maintain a separate accounting when an agency automatically furnishes a copy of a form to another agency each time it prepares one.

Following are examples of automatic disclosures and how they are accounted for.

#### DD Forms 214 and 215

When a military member is separated from active duty, the military departments prepare a DD Form 214--Report of Separation from Active Duty. A DD Form 215 is prepared if a Form 214 is not fully completed or needs to be corrected. Military departments are required to forward copies of these forms to the VA Data Processing Center in Austin, Texas.

Lowry Air Force Base accounts for the disclosure of each DD Form 214 to VA by:

- Preparing punched cards and entering the data into the Air Force-wide Privacy Act Tracking System, which is a computerized system maintained at the Military Personnel Center, San Antonio, Texas.
- Manually making entries on AF Form 771 (Accounting of Disclosures), which is required to be retained at Lowry Air Force Base for 5 years.
- Identifying the distribution to VA on the Form 214, filed in the individual's personnel record (required by Air Force regulation).

The Air Reserve Personnel Center, Denver, Colorado, prepared about 4,400 DD Forms 214 and 215 during the period November 1, 1975, to August 20, 1976. Each automatic disclosure to VA is entered in the Air Force-wide tracking system. Unlike Lowry, the Center does not make an entry on AF Form 771 since the distribution to VA is shown on the Forms 214 or 215 filed in the individual's personnel record. This practice reduces administrative workload and paperwork, and, in our opinion, serves as an accounting of disclosure.

The Fitzsimons Army Medical Center does not make a separate accounting of disclosure when it forwards a copy of the Form 214 to VA. A Fitzsimons official told us an

accounting is not necessary because they can construct the disclosure information if required.

#### DD Form 1343

When it becomes necessary to make a change in a reservist's name, social security number, or date of birth, the Air Reserve Personnel Center completes DD Form 1343--Notification of Change in Service Member's Official Records--and forwards a copy to previous recipients of the information. If the change involves the social security number, a copy is sent to the Social Security Administration. Item 21, "Copy To" of the Form 1343, shows who received copies.

The Form 1343 is a permanent document filed in the reservist's personnel record. The reservist also receives a copy. When the Center forwards a copy Form 1343 to previous recipients, it also makes an accounting of disclosure entry in the Air Force-wide tracking system.

The Form 1343 in the personnel record should, we believe, serve as an accounting of disclosure since the form shows who received copies. Further, the reservist has his or her own copy showing the distribution.

#### QUESTIONABLE VALUE OF ACCOUNTING FOR CERTAIN TYPES OF DISCLOSURES

The Fitzsimons Army Medical Center and Lowry Air Force Base maintain locator card files showing certain information about military members such as name, grade, home address, and home phone number. Both installations list their locator files as systems of records. Members are given the opportunity to give written consent to release, by telephone, their home address and home phone number to any requestor who calls the locator desk. The installations, we were told, do not release the information unless consent is given.

Lowry prepares an accounting of disclosure when it releases information from the locator cards, which includes obtaining the caller's name and address. Fitzsimons, on the other hand, does not prepare an accounting of disclosure.

Lowry Air Force Base's telephone directory contained home addresses and home telephone numbers of base personnel. We contacted an Air Force official in Washington concerned with Freedom of Information Act policy, and were told that all Air Force installation telephone directories have a

section listing home addresses and home phone numbers of all individuals who did not request that this data be withheld. He also said the telephone directories are available to the public under the Freedom of Information Act.

In our opinion, maintaining an accounting for disclosures for locator files where individuals have authorized release of such information as home addresses and home telephone numbers serves no useful purpose and results in unnecessary paperwork. Furthermore, a locator desk has no assurance that callers requesting the information are who they say they are, or that callers have given correct addresses.

COPY FEES VARY  
AMONG AGENCIES

The Privacy Act requires agencies to "establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record." OMB guidelines provide that, in establishing fee schedules, agencies should consider the cost of collecting the fee in determining when fees are appropriate.

Most locations have established fees to charge individuals who request copies of documents from their files. It has been a general practice, however, to waive these fees, if less than a stated minimum, because the administrative burden of collecting the fees is counterproductive. The minimum charges vary among agencies, and at some locations visited they were not applied consistently. Some examples of fee charges at locations visited follow.

- The unit processing requests at DEA charges requestors a fee of \$0.10 per page; however, if the cost totals \$5 or less, the fee is waived, since collecting the fee would be greater than the fee itself. (Department of Justice regulations provide for waiving fees when under \$3.)
- The FBI charges \$0.10 per page, unless the cost totals less than \$3. The fee is waived under \$3.
- The Department of State charges \$0.10 per page, but there is no charge for requests involving \$1 or less.

Air Force Regulations regarding fees are not being applied consistently. The Privacy Act regulation, AFR 12-35, states that normally, copying fees totaling less than \$3 will be waived. Another regulation, AFR 12-32--Schedule of Fees

for Copying, Certifying, and Searching Records and Other Documentary Material--which was in effect before the Privacy Act came into being, sets a minimum copy charge of \$2 for up to six pages and \$0.05 for each additional page.

The policy of the personnel office at Lowry Air Force Base is to waive fees under AFR 12-35 if the requestor cites the Privacy Act. Representatives said, however, that requestors rarely cite the act. If the requestor does not cite the act, the personnel office applies AFR 12-32 and charges \$2 for up to 6 pages and \$0.05 for each additional page. For example, in January 1977, an individual was furnished with 23 copies for \$2.35 (\$2 for 6 copies and \$0.05 for each of 17 additional copies). If he had cited the act, the fee would have been waived. In contrast, the Air Reserve Personnel Center in Denver waives charges of \$3 or less, regardless of whether the individual cites the act.

According to OMB supplemental guidelines, dated November 21, 1975, requests by individuals for access to their own records who do not cite the Privacy Act should be handled under the Privacy Act.

NEED TO PERIODICALLY  
EVALUATE EFFECTIVENESS  
OF STAFF TRAINING

Locations we visited had provided some type of Privacy Act training for employees whose duties were directly affected by the law. These programs included Civil Service Commission courses, Federal Bar Association workshops, in-house courses, question and answer sessions, slide briefings, and films.

The degree of training provided to personnel varied. For example, the Air Reserve Personnel Center provided a wide range of training. Military and civilian personnel assigned to the Center received a Privacy Act briefing, question and answer sessions with supervisory personnel and Privacy Act officers, and small group sessions when requested. The VA Denver Regional Office's Privacy Act officer attended training conducted by the agency in Washington, D.C. He also attended training sponsored locally by the Civil Service Commission and a course sponsored by the Federal Bar Association. He conducted 3 hours of training for all employees of the Denver Regional Office. The General Services Administration Area Personnel Office supervisors attended a centralized training program sponsored by the region. In addition, the regional personnel officer conducted a training session in Kansas City for all employees of the Area Personnel Office who wished to attend.



We made no assessment of the training provided by the locations visited, but it appears that some of the instances of noncompliance found during our review were related to operating personnel's lack of knowledge of the Privacy Act's requirements.

While we found various instances of noncompliance with the act at locations visited, we did not make an in-depth evaluation to determine whether this was due to inadequate training or inadequate implementation of procedures presented during training sessions. It is apparent, however, that Privacy Act implementation should be reviewed periodically to see if staffs are fulfilling the requirements of the act and to determine whether additional training or other action is necessary.

## CHAPTER 3

### LOCATIONS CITE BENEFITS

#### AND PROBLEMS OF THE

#### PRIVACY ACT

During our review at the locations visited, we examined documents relating to Privacy Act implementation, and we discussed with agency officials their experiences and opinions regarding benefits and problems resulting from the Privacy Act, which are summarized in the following sections.

#### BENEFITS

The following benefits were cited as resulting from the Privacy Act.

- The opportunity for individuals to have access to and amend their records, and the deletion of old or possibly derogatory information from the records. For example, one agency official stated that he was aware of three or four cases where individuals reviewed their files and located evidence which had been overlooked by the agency that would lend support to requests for veterans benefits. Prior to the act, individuals were not allowed to have access to their records at this location.
- Greater awareness of the need for protecting personal data from unwarranted disclosure and the proviso for penalties for negligence in protecting information. This should stimulate improvements in recordkeeping and safeguarding measures.
- The destruction of unnecessary systems of records; the consolidation of some systems of records; the elimination of some forms and revision of others to eliminate certain information; the review of information contained in systems of records; the gathering of less personal information than in the past; and greater accuracy of records.
- Members of the public that are asked to furnish information are now advised of whether it is mandatory or voluntary and what the consequences are if the data is not provided.

--The act has provided the intangible benefit of promoting public goodwill and has encouraged employees to review information about themselves in agency personnel files.

While the majority of agencies believe the Privacy Act is beneficial, officials at several locations visited said they thought no major benefits resulted from the act.

### PROBLEMS

The following problems were cited.

- Accounting for disclosures. Officials cited such effects as additional paperwork, increased cost, and increased administrative and legal workload on the existing staff, which detracts from the agencies' primary missions.
- The potential problem of restricting the exchange of information between Federal agencies, between Federal agencies and State and local governments, and between Federal agencies and police departments, for fear of violating the Privacy Act and incurring penalties. This could lessen Government effectiveness and efficiency.
- In addition to the problem of protecting the confidentiality of third parties, the FBI and DEA cited the potential problem of pretrial discovery. Individuals being investigated or slated for trial can request information on themselves from these agencies. Relevant information, if inadvertently disclosed, could jeopardize law enforcement efforts. Another concern is that denying an individual personal information by exemption is a tipoff that the agency has information on the individual that could indicate that he or she is under investigation.

## CHAPTER 4

### CONCLUSIONS AND RECOMMENDATIONS

#### CONCLUSIONS

We believe agencies are making a concerted effort to implement and comply with the Privacy Act. We believe, however, that improvements can be made in how the provisions of the act are being carried out.

We found various instances at the locations reviewed where agencies were not in compliance with the Privacy Act. The noncompliance appeared to result from misinterpretation of the act or guidelines or unfamiliarity with the act. Therefore, we believe there is a need for periodically evaluating the manner in which various agency locations are fulfilling the requirements of the act, to determine if additional training or other action is required.

We believe that the paperwork and administrative workload could be reduced by making greater use of one-time Privacy Act notices or by revising forms to incorporate the notice. Also, agencies should eliminate duplicate systems of accountings for disclosures and the requirement to maintain an accounting for certain types of disclosures.

Costs related to accountings for disclosures in Federal agencies totaled \$9.4 million, or 26 percent of the total operating cost for the Privacy Act, during the year ended September 30, 1976. We believe agencies should evaluate their methods of accounting for disclosures to determine whether this responsibility can be fulfilled in a less costly manner.

#### RECOMMENDATIONS

To insure that agency locations are complying with the Privacy Act, and to reduce the cost of carrying out the provisions of the act, we recommend that OMB:

- Encourage heads of departments and agencies to periodically review the manner in which installations are fulfilling the requirements of the Privacy Act to determine whether additional training or other action is necessary.
- Emphasize to agencies the opportunities for reducing the cost of accounting for disclosures by evaluating their methods of maintaining the accountings, with

a view toward eliminating duplication and unnecessary paperwork.

--Determine whether agencies should be required to maintain accountings for disclosures from locator files where individuals have authorized release of such information.

--Advise agencies to make greater use of one-time Privacy Act notices, where practicable, or revise forms to incorporate the notices.

OMB officials generally agreed with the recommendations and advised us that actions would be taken in accordance with the recommendations.

## CHAPTER 5

### SCOPE OF REVIEW

We reviewed implementation efforts at 28 locations representing 11 civil agencies (20 locations) and at the Department of Defense (8 locations). We reviewed the Privacy Act, OMB guidelines, the Report of the Privacy Protection Study Commission, the Final Summary Report and the Confidentiality and Privacy Report of the Commission on Federal Paperwork, agency policies and procedures for implementation of the Privacy Act, and more specific guidelines from subagency and bureau levels. We also reviewed agency publications in the Federal Register.

At each location, one or more systems of records were selected for examination--the criteria being those systems with the highest rate of inquiry for other than routine use. Systems selected included investigative, medical, driver, loan, claims and collection, and personnel files. We reviewed a few (normally ten or less) individuals' files within one system of records at most locations to see what information was being collected, how it was used, and the disclosure accounting procedures being followed.

We interviewed agency officials directly responsible for implementing the Privacy Act and agency personnel charged with maintaining record systems.

Specific information on the locations covered in our review is shown in Appendix I.

INSTALLATIONS AND LOCATIONSINCLUDED IN THIS REVIEW

<u>Installation</u>	<u>Location</u>
Department of Agriculture: Agriculture Stabilization and Conservation Service Office, Sangamon County Office of Investigation	Springfield, Ill. Washington, D.C.
Civil Service Commission: Bureau of Personnel Investigations	Washington, D.C.
United States Customs Service: Office of Investigations Baltimore Region Office Philadelphia District Office	Baltimore, Md. Philadelphia, Pa.
Department of Defense: Air Reserve Personnel Center Army Aviation Systems Command Army Corps of Engineers District Office Army Reserve Components Personnel and Administration Center Fitzsimons Army Medical Center Lowry Air Force Base Naval Regional Medical Center Philadelphia Naval Shipyard	Denver, Colo. St. Louis, Mo.  St. Louis, Mo.  St. Louis, Mo. Denver, Colo. Denver, Colo. Philadelphia, Pa. Philadelphia, Pa.
General Services Administration: Area Personnel Office National Personnel Records Center, Civilian Personnel Records	St. Louis, Mo.  St. Louis, Mo.
Department of Health, Education, and Welfare: Office of Guaranteed Student Loans Office of Guaranteed Student Loans, Region III St. Elizabeths Hospital	Washington, D.C.  Philadelphia, Pa. Washington, D.C.

InstallationLocation

Social Security Administration: Philadelphia Region Baltimore Headquarters	Philadelphia, Pa. Baltimore, Md.
Department of Labor: Denver Regional Office	Denver, Colo.
Department of Justice: Drug Enforcement Administration Federal Bureau of Investigations Securities and Exchange Commission	Washington, D.C. Washington, D.C. Denver, Colo.
Department of State	Washington, D.C.
Department of Transportation: National Highway Traffic Safety Administration	Washington, D.C.
Veterans Administration: Regional Office Regional Office and Insurance Center	Denver, Colo. Philadelphia, Pa.

(941108)