Office of
INSPECTOR GENERAL

Audit Report

Analysis of the U.S. International Trade Commission's Privacy Act Systems of Records

Report No. IG-01-97

UNITED STATES INTERNATIONAL TRADE COMMISSION

October 1996

INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

October 18, 1996

TO: THE COMMISSION

I hereby submit an *Analysis of the U.S. International Trade Commission's Privacy Act Systems of Records, Report No. IG-01-97*. The Privacy Act of 1974 is the primary federal statute aimed at protecting individual privacy. It imposes government-wide standards on how agencies collect, maintain, use, and disseminate personal information. Each agency is primarily responsible for its own implementation of the Privacy Act in accordance with agency guidelines prepared by the Office of Management and Budget (OMB). Most provisions of the Act apply only to agency records maintained in a system of records from which information is retrieved by name or other individual identifier.

The Commission has Privacy Act notices for five systems of records. Four of these systems date from 1975. The fifth system, covering inspector general records, was added in 1990. All notices are out of date in some respect. The Commission began to prepare notices to amend the existing systems and add two systems in 1996. Both the existing and proposed new system notices were the subject of this analysis.

The objective of this analysis was to conduct a comprehensive and critical review of the Commission's implementation of the Privacy Act. Specific objectives included reviewing existing Privacy Act notices and proposed revisions to determine which systems of records should be retained, established, or reorganized; identifying additional systems of records that need to be established; examining system notices for content, format, and degree of specificity; and determining whether the Commission is in compliance with major provisions of the Act.

This analysis was conducted by Robert Gellman, Privacy and Information Policy Consultant. He found that existing Commission notices contain outdated and/or extraneous information. Common elements of the notices also contain unnecessary differences. In addition, the Commission's Privacy Act rules, which are separate from the notices, are outdated and need to be revised to be more consistent with the Privacy Act. Several Commission forms do not include required Privacy Act notices. The Commission is in compliance with the Act's requirement for maintaining an

accounting of disclosures and with OMB requests for data for Privacy Act reports. However, the Commission did not comply with OMB requirements for regular reviews of Privacy Act activities.

Gellman concurred with the proposed notices that would have deleted one of the existing systems of records, updated the other four systems, and added two new systems. He also identified five additional systems of records that we believe should be established, despite some uncertainty whether the records qualify as Privacy Act systems. He also recommended that Commission Privacy Act notices include a reference to government-wide system notices applicable to Commission records.

The deficiencies at the Commission are at least partially due to the limited awareness of the Privacy Act and its requirements by senior Commission staff, which is not unusual for an agency that conducts no official activities with individuals and engages in little routine Privacy Act business. Until several years ago, the Commission never received a Privacy Act request for access. In addition, the Commission's Privacy Act Officer, the Director of Personnel, understandably has a limited view of his responsibilities which are not defined in federal regulations or Commission policy.

This report documents that the Commission is not in compliance with several requirements of the Privacy Act. The Act includes a criminal penalty for willfully maintaining a system of records without meeting the notice requirement, but there has never been a prosecution under this section. In theory, the Commission's failure to have a notice for all systems of records or accurate notices for existing systems could give rise to liability under the Privacy Act provisions for civil remedies. However, it seems unlikely that any individual could successfully demonstrate the adverse effect that is an essential requirement of a lawsuit. Potential liability can be avoided altogether by updating and republishing Privacy Act system notices and by putting proper notices on forms.

In the draft report, we recommended that the Director of Personnel, in his current capacity as the Commission's Privacy Act Officer, coordinate with the appropriate Commission officials and oversee the implementation of the actions needed to correct the above deficiencies. These actions are stated throughout the report and summarized on page 23.

In his response, the Director of Personnel stated that the threshold issue of deciding who should be the Privacy Act Officer should be addressed first so that whoever is eventually charged with administrative responsibility will have the benefit of participating in the program's implementation. Further, he reported that the Office of General Counsel work to redraft the Commission's systems of records and revised rules is in an advanced stage, which will accomplish the majority of the needed actions identified in our report. His response is presented as an appendix to this report.

The Chairman concurred with the Director of Personnel's response and formed a group under the chairmanship of the Director of Administration to

undertake a review to determine where Privacy Act administration should be assigned. The group is to forward a recommendation to the Chairman by October 31, 1996. Accordingly, we revised the report to recommend that the Director of Administration, in his capacity as chairman of the above mentioned group, notify Committee members of the need to continue working on implementation of the recommendations, and to notify the Privacy Act Officer, when one is designated, of his or her responsibility to respond to the recommendations in the final report. He agreed to take these actions.

Jane E. Altenhofen
Inspector General

TABLE OF CONTENTS

I. Introduction 1
- A. Objectives 1
- B. Scope and Methodology 2

II. Systems of Records Notices 3
- A. Existing Systems: *Retain, Eliminate, or Reorganize?* 3
  - 1. Employment and Financial Disclosure Records 4
  - 2. Budgetary and Payroll-Related Records 4
  - 3. Time and Attendance Records 4
  - 4. Grievance Records 4
  - 5. OIG Investigative Files General and Criminal 4
- B. Proposed New Systems 5
  - 1. Telephone Call Detail Records 5
  - 2. Security Key Use Records 5
- C. Additional Systems of Records 6
  - 1. Security Officer Control Files 6
  - 2. Library Circulation Records 7
  - 3. Parking Records 8
  - 4. Mailing List 8
  - 5. Congressional Correspondence Records 9
- D. Possible Systems of Records 9
  - 1. Activity Accounting 9
  - 2. Web Page 9
  - 3. Locator/Telephone Records 9
  - 4. Administrative Protective Orders 10
- E. Government-Wide Systems 10
- F. Accuracy of System Notices: General Observations 11
  - 1. Common Elements 11
  - 2. Structuring Common Routine Uses 12
  - 3. Adequacy of Existing Common Routine Uses 13
  - 4. Internal Routine Uses 13
  - 5. Descriptions of Policies and Practices 13
- G. Accuracy of System Notice - Specific Comments 15
  - 1. Employment and Financial Disclosure Records 15
  - 2. Budgetary and Payroll-Related Records 15
  - 3. Time and Attendance Records 17
  - 4. Grievance Records 17
  - 5. OIG Investigative Files General and Criminal 17
  - 6. Telephone Call Detail Records 17
  - 7. Security Key Use Records 18

III. Other Privacy Act Requirements 18
- A. Privacy Act Rules 21
- B. Accounting 18
- C. Forms 20
- D. Computer Matching 21
- E. Reporting and Reviewing Requirements 21

F. Personnel Familiarity with the Privacy Act 22
G. Vulnerability Assessment for Litigation 23

IV. Summary of Recommendations 23

Attachment: Suggested Common Routine Uses 25

Notes 29

Appendix: Final Response to Inspector General's Draft Report: Analysis of USITC's Privacy Act Systems of Records, September 30, 1996

ANALYSIS OF THE U.S. INTERNATIONAL TRADE COMMISSION'S
PRIVACY ACT SYSTEMS OF RECORDS

I. Introduction

The United States International Trade Commission (USITC) is an independent federal agency. As with other federal agencies, the Commission is subject to the Privacy Act of 1974.[1] The Privacy Act is a general privacy and records management statute establishing rules and procedures for the collection, maintenance, use, and disclosure of personal information about identifiable individuals. Most provisions of the Act apply only to agency records maintained in a system of records from which information is retrieved by name or other individual identifier.

Major provisions of the Privacy Act require agencies to:

- limit disclosure to those expressly authorized in the statute[2] or through routine uses[3] defined by the agency;
- maintain an accounting for all disclosures;[4]
- allow the subject of a record to have access to and to request amendment of the record;[5]
- inform each individual asked to supply personal information of the purpose and basis for the request;[6]
- publish descriptions of each agency system of records in the Federal Register;[7]
- promulgate rules to carry out the provisions of the Privacy Act;[8]
- establish an administrative mechanism to oversee agency computer matching activities.[9]

A. Objectives

I reviewed Commission's compliance with major requirements of the Privacy Act of 1974 and ongoing activities to update existing system of records notices. Specific objectives were to:

- review existing Privacy Act notices and proposed revisions and determine which systems of records should be retained, established, or reorganized;
- for systems that do not need to be retained, determine whether any other action needs to be taken, such as adopting another agency's system notice;
- for systems that do need to be retained or established, determine the accuracy and/or propriety of all information in the notice;

- identify additional systems of records that need to be established;

- compare system notices for content, format, and degree of specificity;

- determine whether the Commission is in compliance with major provisions of the Act;

- identify agency requirements in OMB Circular A-130 and determine whether the Commission is in compliance and how long the Commission was not in compliance;

- conduct a vulnerability assessment of potential litigation challenges under the Act;

- determine whether the contract with the Commission's security contractor makes provisions of the Act binding on the contractor and its employees;

- evaluate whether Commission personnel are familiar with the requirements of the Act and conduct a vulnerability assessment of potential litigation risks;

- review the circumstances of three open investigations involving potential Privacy Act violations.

B. Scope and Methodology

I conducted a review of the Commission's Privacy Act policies, practices, system notices, and rules during July and August 1996 at USITC headquarters in Washington, DC. The review was conducted in accordance with generally accepted government auditing standards. The review included these elements:

- interviews with managers for each existing and proposed system of records and with the Director of the Office of Personnel, Director of the Office of Finance and Budget, Inspector General, Director of the Office of Management Services, an Assistant General Counsel, Director of the Office of Information Services, Director of the Office of Administration, Secretary to the Commission, Director of the Office of Equal Employment Opportunity, Director of the Office of External Relations, and Director of the Office of Management Services

- examination of existing and proposed[10] Privacy Act system of records notices

- examination of Commission forms that may be subject to Privacy Act notice requirements

- examination of Commission Privacy Act regulations.

This audit relied upon these documents and publications:

- OMB Privacy Act Guidance, 40 Federal Register 28948 (July 9, 1975);

- OMB Circular A-130 on Management of Federal Information Resources, 61 Federal Register 6428 (February 20, 1996) (Appendix I);

• OMB Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974, 48 Federal Register 15556 (April 11, 1983);

• Debt Collection Improvement Act of 1996;

• OMB Guidance on the Privacy Act Implications of "Call Detail" Programs to Manage Employees' Use of the Government's Telecommunications Systems, 52 Federal Register 12290 (April 20, 1987);

• OMB Final Guidance Interpreting the Provisions of Public Law 100-503, Computer Matching and Privacy Protection Act of 1988, 54 Federal Register 25817 (June 19, 1989);

• OPM Republication of Government-Wide System of Records Notices, 61 Federal Register 36919 (July 15, 1996);

• Office of Federal Register, Privacy Act Issuances (1993 Compilation) (CD-ROM).

II. Systems of Records Notices

There are Privacy Act notices for five existing Commission systems of records. Four of these systems date from 1975. The fifth system, covering inspector general records, was added in 1990. All notices are out of date in some respect. The Commission became aware of this and began to prepare amended and additional system notices. Both the existing and proposed new system notices were the subject of this audit.

The Privacy Act gives agencies considerable discretion in defining its systems of records. There is no single right way to define systems. Major factors identified in the OMB Privacy Act Guidelines are the protection of individual rights under the Act the cost and convenience to the agency.[11]

A. Existing Systems: *Retain, Eliminate, or Reorganize?*

1. Employment and Financial Disclosure Records - The Deputy Designated Agency Ethics Official manages this system of records. The system notice contains financial disclosure forms required under ethics laws. A government-wide system notice maintained by the Office of Government Ethics also covers the records.[12]

In the Commission's draft revision of its system notices, this system was to be eliminated in favor of sole reliance on the OGE system. This is appropriate. There is no need to maintain a separate Commission system notice. Reasons to maintain a local system are if it contains additional, locally-provided information not described in the OGE notice or if there is a need for additional routine uses. I found no evidence that either reason is applicable.

Recommendation

Eliminate the Employment and Financial Disclosure Records system notice.

2. Budgetary and Payroll-Related Records - The Office of Finance and Budget manages these records. The system notice reflects an older, paper-driven system used to create both budget and payroll materials. There were two overlapping and parallel systems operated at the same time and by the same office, and this is apparently why one notice covers the budget and payroll records.

The two functions continue, but the operations share an increasingly integrated database. The system should continue to be defined as a Privacy Act system. However, it is appropriate to change the name. The budget uses and any other functions can be explained in the purpose section of the notice. There is no need to reference all of the subsidiary uses in the title. One possible title that might be more descriptive is *Pay, Leave, and Travel Records*. This is the name used by the Office of Personnel Management for its internal payroll system.

3. Time and Attendance Records - The Office of Finance and Budget also manages this system, along with an electronic collection system that pulls in records created by each Commission office. The information is integrated with payroll functions. While it is a matter of choice, there does not appear to be any good reason to continue treating these records as a separate system. Most readers would associate time and attendance records with payroll records. The system can be eliminated and included in a new payroll system notice.

Because of the role now played by the Department of the Interior (DOI) in managing Commission payroll records and functions, a new system notice needs to be properly coordinated with DOI activities. The Overseas Private Investment Corporation (OPIC) is another agency that uses DOI for payroll services, and OPIC has a system notice that reflects its connection with DOI.[13] That notice is a useful model for the USITC system notice. The parts of the OPIC notice most worthy of attention are the System Location (including a reference to the DOI facility) and the Routine Uses.

Recommendation

Merge the Budgetary and Payroll-Related Records with the Time and Attendance Records and establish a new system called *Pay, Leave, and Travel Records*.

4. Grievance Records - The Office of Personnel manages this record system. It is virtually identical to an OPM system (OPM/INTERNAL-11) covering identical records. The OPM grievance system is not a government-wide system so a local system notice is essential. This local system continues in existence and should continue to be defined as a Commission Privacy Act system.

5. OIG Investigative Files General and Criminal - The Office of Inspector General manages this system, which is two systems with a combined system notice. The investigative operations and supporting files continue largely as described in the notice. The system notice should be retained. However, the inclusion of two different exempt systems in a single system notice is inappropriate. Privacy Act exemptions must be system-specific. To be clear, two separate system notices should be promulgated, one for general records and one for criminal records.[14] There is a clear basis for concluding that the Office maintains two separate record systems.

Recommendation

Publish separate system notices to clarify that OIG files are maintained in two distinct systems.

B. Proposed New Systems

Deciding when individually identifiable records form a Privacy Act system of records can be as much an exercise in epistemology as a mixed question of fact and law. The drafters of the Act relied upon mainframe computer records or paper records as a model. Today's modern PC-based and network-resident relational databases make the now ancient legal distinctions difficult to apply in practice. Disagreements about whether records are a formal system occur among Privacy Act experts.

Whether a collection of personally identifiable records qualifies as a Privacy Act system of records is largely a matter of fact. If records within the control of an agency are regularly retrieved by identifier, then they qualify as a system. As a result, deciding whether a computerized database qualifies requires judgment and fact-finding. In a recent D.C. Court of Appeals decision on the Privacy Act, the court noted that "there is no magic number of incidental or *ad hoc* retrievals by reference to an individual's name which will transform a group of records into a system of records keyed to individuals."[15]

When there is doubt, the best general advice is to define a Privacy Act system where individual interests may be adversely affected by the intended uses of the records. Another test is to look at the systems of records established by other agencies. There is no reason for the Commission to be a pioneer in defining systems where others have not. In cases where new forms of records -- such as electronic mail -- have some but not necessarily all of the characteristics of systems, the Commission may wish to await clearer guidance from the Office of Management and Budget. The redraft of the Commission's system notices includes two new system notices.

1. Telephone Call Detail Records - There is some doubt about whether these records are a system of records. Telephone numbers produced through the call detail process are not directly associated with names but with a room number and office. In some -- and perhaps many -- instances, this is sufficient to identify a particular individual.

For this reason, and because of the possibility that call detail reporting may be enhanced in the future, it is advisable to include a system notice. Also, because the records have been used in taking adverse action against individuals, any doubt should be resolved in favor of affording maximum protection to privacy interests. Many agencies have system notices for call detail records.

2. Security Key Use Records - This proposed new system covers records about the use of electronic security keys that control access to the building and its corridors. This system includes surveillance information about agency employees. Although the records are rarely actually retrieved by identifier, a purpose of the system is to permit tracking of individual movements when there has been a security breach or theft. While there is some doubt whether this system must be defined as a system of records, its purpose and potentially intrusive nature support a conclusion that a system notice should be maintained.

The contract (ITC-CN-96-0001) with the Commission's security system contractor does not include the standard Privacy Act clause that triggers application of the Privacy Act's provisions and protections to the records maintained by the contractor. The possibility of adding a Privacy Act clause had been discussed within the Commission and a decision was deferred. The contract should be changed to include a Privacy Act clause when next renewed. The contract is annual, with a series of one-year option years through September 30, 2000. The next renewal date is October 1, 1996.

There is a separate security-related collection of personnel records through the sign-in sheets maintained at the front door to the building. These sheets create records that are equivalent to those created through the security key system. One response is to establish a general system of records for *Security Access Information*. Both the sign-in sheets and the security key records would be part of this single system of records.[16]

Recommendations

Establish a *Security Access Information* system notice covering both electronic and physical security records.

Amend the security contract to include the standard Privacy Act clause when the contract is next renewed.

C. Additional Systems of Records

It is not uncommon for agencies to discover systems of records that had gone unnoticed for years. Finding unreported systems is a difficult task. General questions about record keeping practices inevitably produce negative responses. The only effective method is to ask offices if they maintain specific types of records based on the practices of other agencies.

This method identified several systems of records that the Commission did not publish as Privacy Act systems. For these new system notices, the recommendation includes suggestions about routine uses. Defining routine uses is an art and not a science. The Commission may choose not to employ some recommended routine uses or to add others. There is no single right list of routine uses for a system. New systems notices are recommended for these records:

1. Security Officer Control Files - The Director of the Office of Administration is the Commission's security officer responsible for the granting of security clearances. The process entails collecting information and fingerprints from applicants for security clearances and providing that data to investigators from the Office of Personnel Management. After receiving and reviewing the investigative report, the Commission security officer grants or denies a security clearance. The files generated by this process are maintained in a safe in the Office of Personnel, with access limited to the Director of Administration and a staffer in the Office of Personnel.

There are some complications. First, the main investigative reports in the security file are the product of an investigation conducted for the Commission by OPM. The Commission has a copy of the OPM-created report, and OPM also maintains a copy. The reports in the

possession of OPM are part of OPM system notice OPM/CENTRAL-9, Personnel Investigations Records. The OPM system has been properly exempted from parts of the Privacy Act.

It is apparently the view at OPM that this notice is adequate to cover its reports in the hands of other agencies. OPM considers that it is the owner of the records, and it maintains a *central* and not a *government-wide* system notice. The distinction is that a central notice covers OPM-owned records that may be maintained in other agencies. A government-wide notice covers records dually owned by an agency and by OPM.

However, it is not certain that the OPM central notice is adequate for Commission purposes. If the Commission adds information to the security file other than that described by OPM, then the OPM notice is surely insufficient. More troublesome is the possibility that an aggressive requester could argue successfully that an investigative record exempt from access at OPM might not be exempt in the hands of the Commission. At best, there is some doubt that a court would accept an argument that a record in possession of the Commission used by Commission staff to make significant decisions about an employee's status belongs to OPM and is subject exclusively to the OPM notice.

The issue is not likely to arise unless an individual refused a security clearance needed for continued employment challenges the denial. Even if this is not a likely event, there is a simple way to avoid the possibility of a dispute. The Commission should define its own *Personnel Security Investigative Files* and should apply an exemption to the system. Adopting an exemption requires a formal rule.[17] Exemptions that may be appropriately applied to this system include (k)(1) for classified information and (k)(5) for suitability information. Optionally, exemptions (k)(6) for testing information and (k)(7) for armed services promotion information could be applied, but they may not be necessary.

Second, the government's process for personnel security investigations is changing. Investigative work once done by OPM is now conducted by a private company. In the future, the Commission may use this company for its security investigations. The Commission may also use other government agencies from time to time. A new system notice should cover these possibilities in the general descriptions and routine uses.

Recommendation

Establish a new system of records called *Personnel Security Investigative Files* as an exempt system.

2. Library Circulation Records - The main Commission library has a computer system that tracks books borrowed by agency employees. The records can be and are retrieved by name of employee. Twice a year, the library sends a list of each book borrowed to each employee. This computer system qualifies as a system of records from which information is retrieved by individual identifier and requires a Privacy Act system of records notice.

The law library uses a different system for tracking borrowed books that indexes borrowings by book and not by individual. As a result, the law library system is not a system of records. If the law library procedure changes, it could be a separate system of records or it could be included in a single Commission-wide library system.

There is a recommendation below for restructuring the general routine uses for Commission system notices. The Attachment to this report includes proposed new general routine uses. Most of these general routine uses are unnecessary for this system. However, general routine uses E, H, and I might be applied.

Recommendation

Establish a new system of records called *Library Circulation Records.*

3. Parking Records - The Facilities Support Division of the Office of Management Services maintains employee parking records. It manages a contract with Colonial Parking. Employees submit applications every six months, and the applications are filed alphabetically in a file folder by the name of the primary carpool member. This is a system of records.

From the general routine uses proposed in the Attachment to this report, all are appropriate for this system except D and J. General routine use H covers disclosures to the parking contractor, and there is no need for a separate routine use. No other routine uses appear necessary.

Recommendation

Establish a new system of records called *Parking Records.*

4. Mailing List - The Office of the Secretary maintains a consolidated and computerized mailing list with approximately 3000 names. The list contains predominantly business addresses, but perhaps between one-eighth and one-quarter are home addresses. The list includes telephone numbers as well. The Office uses the consolidated list to address press releases and other agency publications.

There is some uncertainty about whether this list qualifies as a system of records. Information is not retrieved by individual identifier except for the maintenance of the list itself. Some agencies have defined comparable mailing lists as systems, and others have not.

The better choice is to establish a system of records for the list. Because these records relate to non-Commission employees, doubts should be resolved in favor of applying the Act fully. Also, it is likely that the future will bring changes in the methods used for communicating with the Commission's constituency. Mail, fax, email, and online access are likely to be used someday.

A system notice for the mailing list might anticipate change by providing for the possibility that contact information beyond name, address, and telephone number may be collected. This will minimize the need for change in the notice. This system of records requires no routine uses.

Recommendation

Establish a new system of records called *Mailing List.*

5. Congressional Correspondence Records - The Office of External Relations maintains a filing system of congressional correspondence alphabetized by name of members of Congress. This is a system of records. If the file were solely a repository of outgoing correspondence, it might not qualify. But there is some retrieval of the files by name.

Many other agencies have defined congressional correspondence records as Privacy Act systems of records. These systems typically contain incoming correspondence, agency responses, and internal control documents. If general congressional contact information is stored in the file, then it too should be included in the system notice.

Routine uses for a congressional record system are uncertain. Most of the general routine uses in the Attachment are unnecessary, and some other agencies have few defined routine uses. One likely routine use would authorize transfer of a record to another agency. This situation may arise when the Commission receives a congressional inquiry that should have gone to another agency. A routine use can authorize transfer of the inquiry to another agency or entity.

Recommendation

Establish a new system of records called *Congressional Correspondence Records*.

D. Possible Systems of Records

1. Activity Accounting - The Commission's activity accounting program collects, compiles, and prints information by name of employee. This could be defined as a separate system of records. In the alternative, the function could be included within the payroll record system. The Commission has wide discretion in making this choice. The simplest alternative is to make the activity accounting records part of the payroll system. The function should be properly described in the categories of records and purpose sections. The activity accounting records should not require any additional routine uses.

Recommendation

Include activity accounting records within the new *Pay, Leave, and Travel Records* system notice.

2. Web Page - The Commission's Web page does not currently collect identifiable information and retrieve it by individual identifier. The Internet is a highly changeable environment, and information practices are dynamic. Changes in Web page usage could result in creation of a system of records. This bears watching. As long as no personal information is collected, there is no Privacy Act obligation. It may be advisable, however, to include a privacy notice on the page to explain the data collection and use policies to visitors. This is not a legal requirement, but it has been recommended as a courtesy.[18]

3. Locator/Telephone Records - The Office of Management Services produces the Commission's telephone directory from a separate computer file maintained for that purpose. That file could be a separate system of records. However, since the records have no other uses and are not normally retrieved by identifier, defining the file as a system is optional. If the same list came from agency personnel records, no separate notice would be required.

4. Administrative Protective Orders - The Office of the Secretary manages Administrative Protective Orders (APO) issued in connection with investigations. Applicants seeking to obtain restricted information pursuant to the Commission's Rules of Practice and Procedure must complete an APO Application Form. The forms are used to create a service list for each case. A copy of the service list is maintained as well in a separate notebook in chronological order by case name. There is no evidence of any actual retrieval of individual records by name or other identifier. As a result, a system of records does not exist. The possible, occasional retrieval of a form filed by a specific individual by a search of the notebook or case files does not alter this conclusion.

If a violation of an APO is alleged, any related files are maintained as part of the main investigation file and not separately or by individual identifier. If a letter of reprimand is issued to an individual because of a violation of an APO, the letter is placed in the case file and not by the name of the individual. The office maintains a separate tickler file to keep track of the dates when these letters are to be expunged. This too does not appear to qualify as a system of records.

If the Commission were required to undertake a large number of investigations for violations of APOs, it is possible that a formal system of records would be needed. However, while there are a large number of APOs, the number of investigations and the number of reprimands is small. This small number of actions allows the Office of the Secretary to manage the functions without a separate filing system. There is no evidence that the present system was established to circumvent Privacy Act requirements. However, because APO and related records may be used to take adverse actions against individuals, this is a sensitive area. If the filing system changes or if the caseload rises significantly, the need for a formal Privacy Act system should be revisited.

E. Government-Wide Systems

Seven agencies maintain government-wide system of records notices.[19] These include records that the Commission may maintain but that do not necessarily require local system notices. The most "famous" is the Office of Personnel Management system for official personnel files.[20]

These system notices are applicable to Commission files without the need for any action or special notice by the Commission. Nevertheless, to make the Commission's Privacy Act notices more descriptive of the types of records maintained on employees, it would be helpful to include a cross reference to them. Some agencies follow this practice.

One way to accomplish this is through an appendix to the Commission's system notices. The appendix might consist of the names of the government-wide systems with this introduction:

> The Commission maintains some personal records covered by government-wide system of records notices published by other agencies. There may not be actual Commission files in all government-wide systems. This list includes all government-wide system notices known as of the publication date, but any later established government-wide system notices may also be applicable.

Recommendation

Include a reference to government-wide systems of records applicable to the Commission in the publication of Privacy Act system of records notices.

F. Accuracy of System Notices: General Observations

1. Common Elements - Three elements in every Commission system notice that can appropriately be identical are the Notification Procedure, Record Access Procedure, and Contesting Record Procedure. There is unnecessary variability in existing system notices.

Specific wording should, of course, be consistent with Commission Privacy Act rules. This report recommends minor changes to the access rules. The language suggested here is consistent with those recommendations.

> Notification Procedure: Individuals wishing to inquire whether this system of records contains information about them should contact the Director, Office of Personnel, United States International Trade Commission, 500 E Street, SW, Washington, DC 20436. The Director of the Office of Personnel is the Commission's Privacy Act Officer.
>
> Individuals must furnish the following information for their records to be located and identified:
>
> 1. Full name(s).
> 2. Date of birth.
> 3. Social Security Number (for employees).
> 4. Dates of Employment (if applicable).
> 5. Signature.
>
> Record Access Procedure: Individuals wishing to request access to their records should contact the Director, Office of Personnel, United States International Trade Commission, 500 E Street, SW, Washington, DC 20436. The Director of the Office of Personnel is the Commission's Privacy Act Officer.
>
> Individuals must furnish the following information for their records to be located and identified:
>
> 1. Full name(s).
> 2. Date of birth.
> 3. Social Security Number (for employees).
> 4. Dates of Employment (if applicable).
> 5. Signature.
>
> Individuals requesting access must comply with the Commission's Privacy Act regulations on verification of identity (19 CFR part 201).
>
> Contesting Record Procedure: Individuals wishing to request amendment of their records should contact the Director, Office of Personnel, United States

International Trade Commission, 500 E Street, SW, Washington, DC 20436. The Director of the Office of Personnel is the Commission's Privacy Act Officer.

Individuals must furnish the following information for their records to be located and identified:

1. Full name(s).
2. Date of birth.
3. Social Security Number (for employees).
4. Dates of Employment (if applicable).
5. Signature.

Individuals requesting amendment must comply with the Commission's Privacy Act regulations on verification of identity (19 CFR part 201).

The system notice for Grievance Records includes in the Record Access Procedures section a useful preface explaining disclosure policies for grievance records. The preface should be retained for that system.

Recommendation

Standardize, to the greatest extent possible, the common elements of system notices in the publication of Privacy Act system of records notices.

2. Structuring Common Routine Uses - Existing systems share a set of routine uses described in an appendix to the system notices. It is common for agencies to list agency-wide system notices in this fashion. The Commission's appendix of common routine uses is, however, ambiguous. The appendix appears in the system notice list before the Inspector General system notice.[21] It is not clear that the appendix applies to that system as well as those listed before the appendix. In addition, the individual system notices fail to include a specific reference to the routine uses listed in the appendix. The result is some ambiguity in the application of the routine uses to all Commission systems.

The use of a general list of agency routine uses is a good idea. It avoids disparate routine uses for similar purposes. Automatically applying all general routine uses to all systems, however, can create problems and may be unnecessary.

Another way of structuring general routine uses is to create a central list of routine uses applicable to more than one system. Each system notice references appropriate routine uses from the list. A common structure for a central list of routine uses is through a list of "General Routine Uses Applicable to More than One System of Records." This list should appear before the system notices themselves, as the first item in the system of records publication after the table of contents. Each system notice would include as part of the specific routine uses a statement such as: "General Routine Uses A, B, C, & F apply to this system." Additional local routine uses for that system, if any, would follow.

Recommendation

Revise the general routine uses and standardize references to these routine uses in each system notice.

3. Adequacy of Existing Common Routine Uses - Of the six existing common routine uses, the first three are relatively standard ones employed throughout government.[22] Despite the widespread adoption of these routine uses, some rewording is appropriate to meet OMB guidance. See the Attachment for suggested revisions to these routine uses.

The fourth common routine use authorizes disclosures for appeals, complaints, and settlements of personnel actions.[23] This is unobjectionable. The last sentence authorizes disclosure to the Civil Service Commission in connection with evaluation and oversight of Federal personnel management. This is out of date because the Civil Service Commission is now the Office of Personal Management. In addition, this should be identified as a separate routine use because it does not relate to the disclosure in the first part of the routine use.

The fifth common routine use authorizes disclosure of records to "officers and employees of a Federal agency for purposes of audit." This may be too broad and too vague to meet the statutory requirement. A court rejected a routine use permitting disclosure to "federal regulatory agencies with investigative units" because it did not provide adequate notice to individuals about how information might be released and for what purpose.[24]

Because the fifth routine use does not define the term *audit*, it may not be informative enough to provide meaningful notice to individuals. It may also fail to meet the requirement that routine uses be compatible with the purpose for which the information was collected.[25] The notice does not suggest a nexus between the audit and the purpose of collection.

Although the routine use in its present form is questionable, it may still be too limited to accomplish its intended purpose. The routine use only permits disclosure to federal agencies. It would not cover disclosure to private auditors working for the Commission or other federal agencies.

This general routine use is not necessary. The first general routine use broadly supports disclosure to other agencies for investigations of violations or potential violations of law. The Act provides directly for disclosures to the General Accounting Office.[26]

The sixth common routine use permits disclosure to the General Services Administration in connection with administrative services provided by GSA under agreement.[27] These services are now performed by another government agency. This problem can be addressed by making the general routine use more generic.

The Attachment contains a list of suggested general routine uses that might be adopted by the Commission.

4. Internal Routine Uses - Some existing and proposed routine uses authorize disclosure to Commission employees. This is unnecessary and should not be done through a routine use. The Privacy Act authorizes disclosures to officers and employees of the agency maintaining the record who have a need for the record in the performance of their duties.[28] The Commission's General Counsel, Inspector General, and all other agency officials can obtain needed information under this statutory authorization. If a routine use purports to establish a standard for access less stringent than that in the Act, the routine use is improper.

5. Descriptions of Policies and Practices - Each system notice contains specific descriptions of basic records management policies. Many of these descriptions are out-of-date

because of the passage of time and changes in technology. The descriptions should be updated by the system managers, keeping in mind these considerations:

Storage: Technologies used for record storage continue to evolve. Describing storage media with too much precision will only make system notices unnecessarily obsolete. At the same time, there is a clear obligation to describe the media used in order to inform the reader. The nature of the storage medium provides information about the vulnerability of the data to misuse.

In all cases, it will be useful to state whether information is stored on paper or in file folders, in computer media (without necessarily distinguishing between floppy disk, hard disk, tape, etc.), on other media (microform or CD-ROM), or in an online environment. It would also be appropriate to state if records exist on an internal network, are accessible externally or are otherwise shared electronically.

Retrievability: This is the key characteristic that makes a collection of records into a formal Privacy Act system of records. A brief description of how records are retrieved (by name, SSN, etc.) is appropriate.

Safeguards: The general security requirement of the Privacy Act calls for appropriate safeguards.[29] Because almost all Commission records pertain to Commission employees, major threats to security are internal. This is not to diminish the importance of proper security. Misuse of records by insiders is a major threat for almost all personal records. The gossip value of personnel and other records should not be dismissed lightly.

All physical records stored at Commission headquarters are in an environment that generally restricts public access to the offices maintaining the records. This should be noted in each system notice. Additional security measures (e.g., locked or lockable filing cabinets, locked rooms, restricted areas, password protected) for specific systems should also be described accurately. As more records move into the online environment, the Commission should make sure that only those employees who require access to the records can see them, and these measures should be generally described in the relevant system notices.

Each system may have different safeguards and may require slightly different descriptions. As a model, a suggestion for the Inspector General records is offered:

> All Commission records are maintained in a building with restricted public access. The records in this system are kept in a limited access area within the building. The files are maintained in secure file cabinets, and access is limited to persons whose official duties require access.

Retention and disposal: Some proposed system notices refer to records disposal schedules. This is a useful way of addressing the requirement to describe policies for retention, although it is not required by the Act. The goal of the law is to inform the reader how long the records remain at the agency or in other storage. Disposal of unnecessary records offers a significant privacy protection.

When system notices refer to records disposal schedules, some basic details should be included. The general comment that records will be retained and disposed of in accordance with applicable disposal schedules conveys no actual information. Similarly, a reference to a

specific disposal schedule by number conveys little information. An interested reader must seek elsewhere to obtain a copy of the generally obscure disposal schedule. The best result is to state directly how long records are maintained. An additional reference to a disposal schedule is helpful and would encourage compliance with applicable disposal rules.

Access Controls - The statutory requirement for describing policies and practices[30] specifically mentions "access controls" as an element that should be described. The 1975 OMB guidelines describe this as the measures that have been taken to prevent unauthorized disclosure and what categories of individuals within the agency have access.[31]

There is no specific category for access controls in existing notices. This is not necessarily a defect. Many agencies do not include a section for access controls. The subject can be handled through a description included under the *Safeguards* section of the notice.

G. Accuracy of System Notice - Specific Comments

For all existing system notices, the current address for the Commission should be included. Only the Inspector General system includes the correct Commission address.

For all existing system notices, the legal authority for maintenance of the system may need to be updated with references to current law.

For all existing system notices, the descriptions of categories of individuals, categories of records, policies and practices, and record source categories should be rechecked. Specific problems are described below.

1. Employment and Financial Disclosure Records - If this system is eliminated as recommended, then the system notice does not need to be corrected or updated. If retained, the existing routine uses must be revised because they are unclear, out-of-date, and unnecessary.

2. Budgetary and Payroll-Related Records - The *system location* description should state that payroll records are also stored on a computer system operated by the Department of the Interior as well as by the Commission.

The description of *categories of records* is out-of-date. Some specific types of records referenced in the notice no longer exist. The current description is admirably specific but more detailed than necessary. A generic description of the information maintained rather than the specific ways in which the records are organized would be appropriate and less likely to become obsolete. This example from OPM/INTERNAL-5 covering Pay, Leave, and Travel Records offers one model:

> This system contains various records relating to pay, leave, and travel. This includes information such as: Name; date of birth; Social Security Number; home address; grade; employing organization; timekeeper number; salary; pay plan; number of hours worked; leave accrual rate, usage, and balances; Civil Service Retirement and Federal Retirement System contributions; FICA withholdings; Federal, State, and local tax withholdings; Federal Employee's Group Life Insurance withholdings; Federal Employee's Health Benefits withholdings; charitable deductions; allotments to financial organizations; garnishment documents; savings bonds allotments; union and

management association dues withholding allotments; travel expenses; and information on the leave transfer program and fare subsidy program.

If any specific element is inappropriate (e.g., fare subsidy program) then it should be dropped. If other elements are part of this system (e.g., activity reporting records), then these elements should be added.

The *authority for maintenance* of the system could be improved. A reference to an entire title of United States Code as authority is unnecessarily vague. The specificity of the OPM notice for a comparable system of records is noteworthy and may offer a useful guide:

> 31 U.S.C. 66a; 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq., and 6301 et seq.; Executive Order 9397; Pub. L. 100-202, Pub. L. 100-440, and Pub. L. 101-509.

The proposed revision of the system notices adds a *purpose* section. This is a highly advisable improvement. The proposed statement of purpose might be useful in this form:

> The Commission uses the records to administer pay, leave, and travel requirements and to prepare the budget.

The *routine use* section should be revised. Suggested routine uses are:

> The records in this system of records are transmitted electronically by the Commission to the Denver Administrative Services Center, U.S. Bureau of Reclamation, U.S. Department of Interior, which provides payroll services. The USITC, and the Department of Interior acting on behalf of the USITC, may make the following routine uses:
>
> a. General Routine Uses A, B, C, D, E, F, G, H, I, and J;
>
> b. To the Department of the Treasury to issue checks and U.S. Savings Bonds;
>
> c. To the Office of Personnel Management for retirement, health and life insurance purposes, and to carry out OPM's government-wide personnel management functions;
>
> d. To the National Finance Center, Department of Agriculture, for the Thrift Savings Plan and Temporary Continuation of Coverage;
>
> e. To the Social Security Administration for reporting wage data in compliance with the Federal Insurance Compensation Act;
>
> f. To the Internal Revenue Service and to State and local tax authorities for tax purposes, including reporting of withholding, audits, inspections, investigations, and similar tax activities;
>
> g. To officials of labor organizations recognized under 5 U.S.C. Chapter 71 for the purpose of identifying USITC employees contributing union dues each pay period and the amount of dues withheld.

The *storage* description in the revised system notice is out-of-date.

The *retrievability* description should refer only to name and social security number. Dates are not identifiers under the Privacy Act.

The *retention and disposal* description is too general. The reference to record disposal schedules without the actual preservation time conveys no useful information to the reader.

The *record source categories* description might be modified to read:

> Information in this system of records comes from the individual to whom the record pertain, Commission officials responsible for pay, leave, and travel requirements, and official personnel documents.

3. Time and Attendance Records - If this system is consolidated with the payroll system, the notice will be eliminated.

4. Grievance Records - The revised notice for this system is generally correct. The routine uses should refer to all general routine uses except D. Proposed routine use 5 (to officials of labor organizations) may be unnecessary if these disclosures can be made with the consent of the record subject. The general routine uses cover other necessary disclosures.

5. OIG Investigative Files General and Criminal - As discussed above, this system should be published as two separate systems of records. Much of the description in the two systems will be similar or identical. However, the *categories of individuals* description should not include a reference to Commission offices and subdivisions. The Privacy Act applies only to individuals and not to legal persons.

The preamble to the *routine use* section should be dropped. It is unclear that the Inspector General can or should seek assurances that recipients of information must comply with Privacy Act safeguards. This language could cause unnecessary liability if a recipient misuses data. The Act's requirements for contractors should be followed when appropriate, but there is no need to include a broader statement responsibility in the routine uses.

In place of the specific routine uses, the notice should include a reference to all general routine uses. There is no need for a routine use covering disclosure to the General Counsel of the Commission (proposed routine use 9). The Privacy Act authorizes necessary internal disclosures.

The proposed routine use does not include a *purpose* section. This should be added to conform with other system notices.

The description of *storage* policy should be made more generic by referring to computer media rather than computer disks.

6. Telephone Call Detail Records - This is a proposed system notice for a newly defined system of records. The *categories of individuals* and *categories of records* descriptions make no reference to the collection of information about local calls. This is accurate since that information is not currently collected. If there is a reasonable prospect that this information

might be collected and maintained in the future, the descriptions might be made more generic to include local calls. This would avoid the need for a possible future change in the notice.

The *routine uses* for this system should incorporate all of the general routine uses except D and J. The first proposed routine use (to a telecommunications carrier) is unnecessary since general routine use H covers contractors. The second routine use (to the Internal Revenue Service) is appropriate, but it might be revised to refer to "other federal agencies or federal contractors with statutory authority to assist in the collection of Commission debts." This will cover the possibility that debt collection functions now conducted by the IRS might be shifted elsewhere. The proposed routine use to the Inspector General is unnecessary.

The *storage* description appears incomplete. Some information is collected on computer tape, and a more general description of the media may be needed.

The *retention and disposal* description is not sufficiently detailed. It should indicate the approximate length of time that the records will be kept.

7. Security Key Use Records - If this newly proposed system is expanded to include physical security records, as suggested above, then the system notice will need to be rewritten and expanded. Appropriate general routine uses for this system are all except D and J. No other routine uses may be needed.

Recommendation

Reexamine and revise each system notice to reflect current conditions and to correct identified deficiencies.

III. Other Privacy Act Requirements

A. Privacy Act Rules

The Commission's Privacy Act rules appear at 19 CFR §201.22-.32 (1995). The rules were originally promulgated in 1975, shortly after the effective date of the Act.[32] A 1990 amendment added exemptions for systems of records maintained by the Inspector General.[33] There are some problems with the existing rules:

• The rules include the former address of the Commission at 701 E Street. The address needs to be updated.

• The rules contemplate that any individual seeking access to his or her records must make an appointment with the Director of Personnel to inspect the records.[34] Alternatively, the Director *may* provide the individual with a copy of the record by certified mail.[35]

The Act clearly provides that an individual may review and have a copy made of all records about himself or herself.[36] The rules should be revised to clarify that a requester has a right to have a copy of a record and to explain more clearly the procedure for obtaining that copy without a personal visit. There is no evidence that this minor deficiency in the rules has adversely affected any actual request.

• The rules provide that fees for copying of records shall be at the rate of ten cents per page. There is no charge unless the total amount exceeds fifty cents.

Under the Freedom of Information Act, no fees may be charged for the first 100 pages of duplication[37] or where the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee.[38] While the FOIA fee standards are not directly applicable to Privacy Act requests, it is common for first-party requests for records to be treated as if the request was made under both laws and for the requester to be charged only the most favorable fees permitted under either law. At a minimum, it would be appropriate for the Commission to conform its Privacy Act fees to the FOIA standards.

An agency need not charge copying fees at all under the Privacy Act, and the Commission may wish to consider not charging for routine requests. The cost of accounting for occasional payments is likely to exceed the cost of processing. Since most Commission records pertain to its employees, a useful policy might be to allow each employee a free copy of his or her personnel file once a year and whenever a change is made.

• There are exemptions in the rules[39] for some systems of records. The exemptions for the Inspector General systems were properly claimed.

The remaining three exemptions are not properly claimed. The Act requires that exemptions be applied to identifiable systems of records. Subsection (a) of the rules invokes an exemption for classified records, but it fails to apply the exemption to a specific system of records. No existing systems appear to contain classified information. As a result, this claim of exemption is both improper and unnecessary.

Subsection (b) of the Commission's rules invokes an exemption for statistical records. Here too, there is no specific system referenced, and no defined system appears to include statistical records. As a result, this claim of exemption is both improper and unnecessary.

Subsection (c) invokes the exemption for investigatory material compiled for determining suitability for employment, federal contracts, and other purposes. The rules apply the exemption to "[p]ersonnel investigations records in the custody of the Security Officer . . . " No specific system is identified, and no existing system appears to include these records. There is a government-wide system of records (OPM/GOVT-5 Recruiting, Examining, and Placement Records) that covers this category of records that already has an exemption. As a result, the exemption claim is both improper and unnecessary.

Recommendation

Revise the Commission's Privacy Act rules.

B. Accounting

The Privacy Act requires that agencies maintain an accounting of the date, nature, and purpose of most external disclosures of records. The name and address of the person or agency receiving the records must also be recorded.[40] No accounting is required for internal disclosures or for disclosures under the Freedom of Information Act. The law does not require maintenance of a specific record, notation, or log of each disclosure. It is sufficient if an agency can reconstruct the accounting from available information when requested.[41]

Only some Commission personnel are aware of the law's accounting requirement. No one reported the maintenance of any specific accounting records. However, it also appears that the routine conduct of agency business either generates records of disclosures or otherwise permits the reconstruction of the accounting for a specific record. The current practices appear sufficient to meet the law's requirement.

When new systems of records are established or existing systems are changed, system managers should consider how the Act's accounting requirement can be fulfilled. As more records become digital, extra care should be taken to make sure that the required accounting for external disclosures can be reconstructed routinely.

C. Forms

The Privacy Act requires that an agency disclose certain information to individuals asked to provide personal data.[42] The Privacy Act notice must appear on the form or on a separate piece of paper.[43] While the Commission staffer responsible for forms automation was aware of this requirement, most other personnel were not. A review of the agency forms list confirmed that no notice appears necessary. However, the list does not reflect all forms in use at the Commission.

Several Commission forms require disclosure of personal information without providing the necessary Privacy Act notice. There is no systematic way to identify these forms, but I was able to find forms that require notices.[44]

• Application--Parking Space (Office of Management Services, USITC #11) - This form calls for a variety of personal information, including home address, and vehicle identification information. This clearly requires a Privacy Act notice. The form itself, however, contains a questionable applicant certification.[45]

• Office of the Secretary Mailing List Form (no title or number) - This form calls for disclosure of the requester's name, address, and telephone number. There should be a Privacy Act notice on the form. In addition, the Office of the Secretary issues a yearly renewal notice asking for confirmation and updating of the same information from requesters. A Privacy Act notice should be added to this form as well.

• Official Travel Authorization (ITC Form 005) - This basic travel authorization form becomes part of the payroll system of records (which contains travel documentation). It requires a Privacy Act Notice. Other travel forms in use include Exceptions to the Use of Contract Carriers (ITC Form 125), Justification for Premium Class Travel (ITC Form 349), Justification for Use of a Foreign Flag Air Carrier (no number), and Justification for Actual Subsistence Travel (ITC Form 350). These forms also need Privacy Act notices.

• Designation of Employee Check (Office of Finance and Budget, ITC Form 351) - This form asks departing employees to disclose social security number and home address. It requires a Privacy Act notice. Presumably, the information is maintained as part of the payroll system of records.

• Security Sign-In Form - Visitors to the building must sign in at the front security desk. A Privacy Act notice should be provided. Since printing the notice on the form itself would

be cumbersome, the requirement can be met by printing the notice on a separate piece of paper and posting a sign that the notice is available upon request.

Recommendation

Add a Privacy Act notice to Commission forms as required by the law.

D. Computer Matching

The Privacy Act imposes requirements on agencies that conduct computer matching or that provide data for other agencies to use for computer matching. I found no evidence that the Commission engages in matching activities as either a source or recipient agency. As a result, the Commission has no current computer matching obligations under the Act.

Personnel information routinely provided to the Office of Personal Management is used in matching, but OPM is the source agency and complies with the requirements of the Act. The Commission also shares payroll and personnel information with its payroll contractor, the Department of Interior. I found no reason to believe that the Department was using Commission data for computer matching purposes. However, if the Department in its role as contractor for other agencies begins to provide data for matching purposes, the Commission may be obliged to create a Data Integrity Board[46] and enter into matching agreements.[47] It might be advisable for the Commission to expressly tell the Department to seek advance approval from the Commission before using personnel data for computer matching.

E. Reporting and Reviewing Requirements

OMB Circular A-130 on the Management of Federal Information Resources lists many reporting and reviewing requirements for agencies subject to the Privacy Act. Agencies must conduct regular reviews of contracts (every two years), recordkeeping practices (every two years), routine uses (every four years), exemptions (every four years), matching programs (annually), training (every two years), violations (every two years), and system notices (every two years). None of these reviews had been conducted. The annual review for matching programs is not applicable to the Commission because there are no matching activities.

Agencies must also provide several different Privacy Act reports. These include the Privacy Act report to OMB (every two years), matching activity report (every two years), new system of records report (when needed), altered system of record report (when needed), and four different types of matching reports. The Commission has had no obligation to file any matching report.

The Commission has complied with other reporting requirements. Reports were filed with the Congress and OMB for the only new system of records adopted in the last twenty years. The Commission also published required Federal Register notices. While the Commission has not kept its Privacy Act system notices up to date, the procedural requirements for adopting new systems were followed correctly.

F. Personnel Familiarity with the Privacy Act

Senior Commission staff interviewed for this audit showed limited awareness of the Privacy Act and its requirements. This is not unusual for an agency that conducts no official activities with individuals and that engages in little routine Privacy Act business. Until several years ago, the Commission never received a Privacy Act request for access.

The Commission's Privacy Act Officer is the Director of Personnel.[48] Based on existing policy, he has limited responsibilities. He serves as the public point of contact for Privacy Act matters and as internal coordinator of Privacy Act requests. In addition, the Privacy Act Officer responds to occasional data calls from the Office of Management and Budget. These functions have been carried out adequately.

The Commission has not assigned responsibility for reviewing system notices, forms, for reminding other staff about Privacy Act obligations for new systems of records, or for investigating complaints. The Commission certainly does not require a full-time Privacy Act Officer to carry out these functions. However, there is a need for someone to undertake general responsibility for overseeing the system notice and form requirements of the Act and for investigating identified problems.

Given the limited number of Privacy Act systems of records maintained by the Commission, an occasional review of compliance is appropriate. One way to accomplish this is to rely upon the biennial data call from the Office of Management and Budget as a prompt. Every two years when OMB asks for Privacy Act reporting information, the Privacy Act Officer should send a copy of each existing system notice to each system manager and ask for a review of the currency of the notice. Any necessary changes can be made then.

This process will help to assure that system notices do not languish another twenty years without updating. If new systems of records are created in the interim (or if there are major changes in existing systems), the notices should be updated more frequently. New routine uses will also require prompt attention. For minor changes, however, revision of system notices every two years is sufficient. A biennial review would also meet all of the review requirements in OMB Circular A-130. Most of the review requirements are biennial. Those required every four years could be conducted easily and quickly biennially.

In addition, Commission staff with responsibility for designing or controlling forms should be alerted to the general requirements of the Privacy Act relating to the creation of forms. They should serve as an early warning system when new forms create Privacy Act obligations. Similarly, Commission staff responsible for designing and maintaining computer systems should be aware of what constitutes a system of records so that they can alert the Privacy Act Officer when possible new systems are created. They should be notified of these general oversight responsibilities immediately and again once every two years.

The Privacy Act imposes a variety of obligations on federal agencies. Once basic compliance is reestablished, it will take little effort to keep current.

Recommendation

Set forth the duties of the Privacy Act Officer to oversee and coordinate the Commission's implementation of the Act, including reviewing existing system notices every

two years when the Office of Management and Budget collects information for the Privacy Act report to Congress, and investigating Privacy Act complaints and known or suspected deficiencies.

G. Vulnerability Assessment for Litigation

This report documents that the Commission is not in compliance with several requirements of the Privacy Act. The Act includes a criminal penalty for willfully maintaining a system of records without meeting the notice requirement.[49] Any potential violation of this section would have to satisfy the *willful* test, and this is unlikely. Many other agencies (including OMB!) are also in technical violation of the publication requirements of the Act. In any event, there has never been a prosecution under this section. The crime is a misdemeanor.

The Privacy Act provides civil remedies[50] that could result in liability. Most Privacy Act litigation is over denial of access or correction or improper disclosures. Suits may also be brought for failure to maintain records with accuracy, relevance, timeliness, or completeness as is necessary to assure fairness. Finally, suits may be brought for any other violation.

In theory, the Commission's failure to have system of records notices for all systems or accurate notices for existing systems could give rise to liability. Given the actual deficiencies found, however, it seems unlikely that any individual could successfully demonstrate the adverse effect[51] that is an essential requirement of a lawsuit. This is also likely to be true for failure to include notices on forms. Unauthorized disclosures provide other grounds for liability, but the adverse effect threshold is hard to overcome in most cases.

It is unlikely that the Commission would be held civilly or criminally liable for most if its failure to comply with Privacy Act requirements. Potential liability can be avoided altogether by updating and republishing Privacy Act system notices and by putting proper notices on forms.

IV. Summary of Recommendations

We recommend that the Director of Administration, in his capacity as chairman of the group formed to undertake a review to determine where Privacy Act administration should be assigned, notify (1) group members of the need to continue working on implementation of the recommendations; and (2) the Privacy Act Officer, when one is designated, of his or her responsibility to respond to the following recommendations:

Eliminate the Employment and Financial Disclosure Records system notice.

Merge the Budgetary and Payroll-Related Records with the Time and Attendance Records and establish a new system called *Pay, Leave, and Travel Records*.

Publish separate system notices to clarify that OIG files are maintained in two distinct systems.

Establish a *Security Access Information* system notice covering both electronic and physical security records.

Amend the security contract to include the standard Privacy Act clause when the contract is next renewed.

Establish a new system of records called *Personnel Security Investigative Files* as an exempt system.

Establish a new system of records called *Library Circulation Records*.

Establish a new system of records called *Parking Records*.

Establish a new system of records called *Mailing List*.

Establish a new system of records called *Congressional Correspondence Records*.

Include activity accounting records within the new *Pay, Leave, and Travel Records* system notice.

Include a reference to government-wide systems of records applicable to the Commission in the publication of Privacy Act system of records notices.

Standardize, to the greatest extent possible, the common elements of system notices in the publication of Privacy Act system of records notices.

Revise the general routine uses and standardize references to these routine uses in each system notice.

Reexamine and revise each system notice to reflect current conditions and to correct identified deficiencies.

Revise the Commission's Privacy Act rules.

Add a Privacy Act notice to Commission forms as required by the law.

Set forth the duties of the Privacy Act Officer to oversee and coordinate the Commission's implementation of the Act, including reviewing existing system notices every two years when the Office of Management and Budget collects information for the Privacy Act report to Congress, and investigating Privacy Act complaints and known or suspected deficiencies.

The Privacy Act Officer will need to coordinate with the appropriate Commission officials to implement the above recommendations, and some actions will require approval by the Commission.

Suggested Common Routine Uses

General Routine Uses Applicable to More than One System of Records

A. Disclosure for Law Enforcement Purposes

Information may be disclosed to the appropriate Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the information indicates a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the receiving entity.

B. Disclosure Incident to Requesting Information

Information may be disclosed to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested), when necessary to obtain information relevant to an agency decision concerning retention of an employee or other personnel action (other than hiring), retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit.

C. Disclosure to Requesting Agency

Disclosure may be made to a Federal, State, local, foreign, or tribal or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

D. Disclosure to Office of Management and Budget

Information may be disclosed to the Office of Management and Budget at any stage in the legislative coordination and clearance process in connection with private relief legislation as set forth in OMB Circular No. A-19.

E. Disclosure to Congressional Offices

Information may be disclosed to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of the individual.

F. Disclosure to Department of Justice

Information may be disclosed to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which the Commission is authorized to appear, when:

1. The Commission, or any component thereof; or
2. Any employee of the Commission in his or her official capacity; or

3. Any employee of the Commission in his or her individual capacity where the Department of Justice or the Commission has agreed to represent the employee; or

4. The United States, when the Commission determines that litigation is likely to affect the Commission or any of its components

is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the Commission is deemed by the Commission to be relevant and necessary to the litigation provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.

G. Disclosure to the National Archives

Information may be disclosed to the National Archives and Records Administration in records management inspections.

H. Disclosure to Contractors, Grantees, etc.

Information may be disclosed to contractors, grantees, consultants, or volunteers performing or working on a contract, service, grant, cooperative agreement, job, or other activity for the Commission and who have a need to have access to the information in the performance of their duties or activities for the Commission. This includes federal agencies providing payroll, management, or administrative services to the Commission. When appropriate, recipients will be required to comply with the requirements of the Privacy Act of 1974 as provided in 5 U.S.C. §552a(m).

I. Disclosures for Administrative Claims, Complaints and Appeals

Information from this system of records may be disclosed to an authorized appeal grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator or other person properly engaged in investigation or settlement of an administrative grievance, complaint, claim, or appeal filed by an employee, but only to the extent that the information is relevant and necessary to the proceeding. Agencies that may obtain information under this routine use include, but are not limited to, the Office of Personnel Management, Office of Special Counsel, Merit Systems Protection Board, Federal Labor Relations Authority, Equal Employment Opportunity Commission, and Office of Government Ethics.

J. Disclosure to the Office of Personnel Management

Information from this system of records may be disclosed to the Office of Personnel Management pursuant to that agency's responsibility for evaluation and oversight of Federal personnel management.

K. Disclosure in Connection with Litigation

Information from this system of records may be disclosed in connection with litigation or settlement discussions regarding claims by or against the Commission, including public filing with a court, to the extent that disclosure of the information is relevant and necessary to the litigation or discussions and except where court orders are otherwise required under section (b)(11) of the Privacy Act of 1974, 5 U.S.C. §552a(b)(11).

*****

Another type of disclosure must be provided for in some Commission systems, but it cannot be accomplished through a routine use. Disclosures of information to consumer reporting agencies pursuant to debt collection laws must be provided for in system notices as appropriate. This cannot be accomplished in a general fashion. Following the routine use section for each applicable system, this section should be included:

> Disclosure to Consumer Reporting Agencies: Information from this system of records may be disclosed to a consumer reporting agency as provided in 31 U.S.C. §3711.

This disclosure authorization section should be included in the system notice for *Pay, Leave, and Travel Records*. The same notice should be added to any other Commission system likely to give rise to claims by the government.

Notes on the Litigation Routine Use

The Privacy Act provides directly for disclosures of records pursuant to the order of a court of competent jurisdiction.[52] This provision has a troubled implementation history, with a good deal of litigation over its meaning. As a result, it is difficult to be definitive about the best way to address disclosures incident to litigation.

Some things are clear. Disclosures can be made when there is a court order signed by a judge. A grand jury subpoena (which is not signed by a judge) does not qualify. A court order signed by the court clerk does not qualify. A routine discovery request from opposing counsel is not a court order unless signed by a judge.

Some agencies tried to avoid these limitations by promulgating routine uses covering these types of disclosures. These routine uses were struck down when challenged.[53] While agencies have considerable discretion in establishing routine uses, they may not promulgate a routine use that would evade or weaken the statutory conditions of disclosure such as (b)(11). Many objectionable routine uses remain in place because they have never been challenged by litigants or revised by the agencies.

Other uncertainties arise when disclosures are incident to administrative adjudications. The (b)(11) limitation on disclosure does not appear to apply at the administrative level, although this is not entirely free from doubt. Still, the Act clearly contemplates interagency transfers of files through routine use, and it would be troublesome and convoluted to conclude that all administrative adjudications require court orders.

Also, if settlement of a claim is being negotiated before the actual filing of litigation, it appears that necessary disclosures can be accomplished through a routine use. No court order can be obtained without the formal filing of a lawsuit so there would be no other way to make these disclosures that may be necessary to protect important government interests.

Routine use 7 proposed for the Inspector General record system, which addressed litigation disclosures, is too broad.[54] There are many existing litigation routine uses of other agencies that are also too broad. While many routine uses can be "validated" by reference to the practice of other agencies, this area is too changeable to rely heavily on other Privacy Act

system notices. General Routine Use K for disclosure in connection with litigation can substitute for the proposed Inspector General litigation routine use.

For some litigation-related disclosures, routine uses are unnecessary. For any case before a court, parties seeking Privacy Act information can and must seek a court order to support the disclosure. Where the attorney for the other side represents the individual who is the subject of a file, that individual's file can be disclosed with consent.

Disclosure of records to the Justice Department when it is representing the Commission in litigation is permissible through a routine use. Proposed General Routine Use F covers this category of disclosures. A routine use is needed to permit the nonconsensual public filing of Privacy Act records with a court. Proposed routine use K covers this category of disclosure.

There may be circumstances in which opposing counsel seeks (or the Commission may wish to disclose) Privacy Act records of individuals who are not parties to the lawsuit. For example, there could be a demand for the disclosure of all personnel files in a particular office to adjudicate or resolve a claim of discrimination. The proposed general litigation routine use protects the ability of the Commission to make any litigation-related disclosures that can be lawfully made through a routine use. All actual disclosures under this authority will require case-by-case review to make sure that the routine use disclosure does not usurp authority reserved to the court under section (b)(11). Whenever possible, non-identifiable or encrypted information may serve the purpose without raising any privacy concerns.

Notes

1. 5 U.S.C. §552a (1994).

2. Id. at §552a(b).

3. Id. at §§552a(a)(7) & (b)(3).

4. Id. at §552a(c).

5. Id. at §552a(d).

6. Id. at §552a(e)(3).

7. Id. at §552a(e)(4).

8. Id. at §552a(f).

9. Id. at §552a(o) & (u).

10. The draft revision of Commission Privacy Act notices reviewed for this audit was dated 3/25/96.

11. 40 Federal Register 28952 (July 9, 1975).

12. OGE/GOVT-1 - Public Financial Disclosure Reports; OGE/GOVT-2 - Confidential Statements of Employment and Financial Interests.

13. See 61 Federal Register 25239 (May 20, 1996).

14. The criminal investigatory records are exempt under a general exemption, 5 U.S.C. §552a(j)(2) (1994). The general investigatory are exempt under specific exemptions, 5 U.S.C. §552a(k)(2) (1994). The Commission rules claiming these records already properly treat the Inspector General records as two separate systems.

15. *Hencke v. Department of Commerce*, No. 95-5195 (D.C. Cir., May 17, 1996).

16. Whether sign-in sheets are records within the purview of the Privacy Act is not without doubt. In *American Federation of Government Employees v. NASA*, 482 F. Supp. 281 (S.D. Tex. 1980), the court held that a daily employee time sheet was held not to be a record that the Congress intended to cover by the Privacy Act. That result is controversial and may not cover the sign-in records at issue here. In the case, the records covered employees only. The Commission's records cover mostly visitors to the Commission's offices, but some employees may be included as well.

17. 5 U.S.C. §552a(k) (1994) ("The head of any agency may promulgate rules . . . to exempt any system of records within the agency . . .").

18. See Gellman, "Action for Privacy Can Force Cookies to Crumble", *Government Computer News* 35 (May 27, 1996).

19. The last publication of a complete list of these notices was at 56 Federal Register 28178 (June 19, 1991).

20. The government-wide systems are:

- EEOC/GOVT-1 - Equal Employment Opportunity in the Federal Government Complaint and Appeal Records.

• FEMA/GOVT-1 - National Defense Executive Reserve System
• GSA/GOVT-2 - Employment Under Commercial Activities Contracts
• GSA/GOVT-3 - Travel Charge Card Program
• GSA/GOVT-4 - Contracted Travel Service Program
• DOL/ESA-13 - Employment Standards Administration, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File
• DOL/ETA-14 - Employment Training Administration (ETA) Job Corpsman Records
• MSPB/GOVT-1 - Appeal and Case Records
• OGE/GOVT-1 - Executive Branch Public Financial Disclosure Reports and Other Ethics Program Records
• OGE/GOVT-2 - Confidential Statements of Employment & Financial Interests
• OPM/GOVT-1 - General Personnel Records
• OPM/GOVT-2 - Employee Performance File System Records
• OPM/GOVT-3 - Records of Adverse Actions and Actions Based on Unacceptable Performance
• OPM/GOVT-5 - Recruiting, Examining, and Placement Records
• OPM/GOVT-6 - Personnel Research and Test Validation Records
• OPM/GOVT-7 - Applicant -- Race, Sex, National Origin and Disability Status Records
• OPM/GOVT-9 - File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals.
• OPM/GOVT-10 - Employee Medical File System Records

21. See 5 Privacy Act Issuances 85-89 (1991). On the 1993 CD-ROM version of Privacy Act Issuances, the appendix is appropriately included after all of the system notices.

22. The text of these routine uses is:

• In the event that a system of records maintained by this agency to carry out its functions indicates a violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a "routine use," to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

• A record from this system of records may be disclosed as a "routine use" to a Federal, State or local agency maintaining civil, criminal or other pertinent information, such as current licenses, if necessary, to obtain information relevant to an agency decision concerning the hiring or retention of any employee, the issuance of a security clearance, the letting of a contract or the issuance of a license, grant or other benefit.

• A record from this system of records may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision in the matter.

23. The text of the routine use is:

• A record from this system of records may be disclosed to an authorized appeal grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee. A record from this system of records may be disclosed to the United States Civil Service Commission in accordance with the agency's responsibility for evaluation and oversight of Federal personnel management.

24. *Britt v. Naval Investigative Service*, 886 F.2d 544 (3rd Cir. 1989).

25. 5 U.S.C. §552a(b)(3) (1994).

26. Id. at §552a(b)(10).

27. The text of the routine use is:

> A record from this system of records may be disclosed to officers and employees of the General Services Administration in connection with administrative services provided to this agency under agreement with GSA.

28. 5 U.S.C. §552a(b)(1) (1994).

29. Id. at §552a(e)(10) ("establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.").

30. Id. at §552a(e)(4)(E).

31. 40 Federal Register 28964 (July 9, 1975).

32. 40 Federal Register 47976 (October 10, 1975).

33. 55 Federal Register 40379 (October 3, 1990).

34. 19 CFR §201.25 (1995).

35. Id. at §201.25(d).

36. 5 U.S.C. §552a(d)(1).

37. Id. at §552(a)(4)(A)(iv)(II).

38. Id. at §552(a)(4)(A)(iv)(I) (1994).

39. 19 CFR §201.32 (1995).

40. 5 U.S.C. §552a(c) (1994).

41. See OMB Privacy Act Guidelines, 40 Federal Register 28956 (July 9, 1975).

42. Subsection (e)(3) provides that each agency shall --

> (3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual --
>
> (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
>
> (B) the principal purpose or purposes for which the information is intended to be used;
>
> (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and
>
> (D) the effects on him, if any, of not providing all or any part of the requested information.

5 U.S.C. §552a(e)(3) (1994).

43. There is case law holding that the notice must be specific in describing the routine uses that apply to the system of records for which information is being collected. The degree of specificity is not entirely clear, and legal judgments are required about the sufficiency of the disclosure. See *Covert v. Harrington*, 876 F.2d 751 (9th Cir. 1989) and *United States v. Wilber*, 696 F.2d 79 (8th Cir. 1982).

44. The Commission uses many standard government-wide forms in the conduct of its business. These forms originate with other agencies (e.g., Office of Personnel Management). The forms that I saw contained Privacy Act notices. It is appropriate for the Commission to rely on the notices prepared by other agencies and on their judgment about the need for and content of Privacy Act notices on these standard forms.

45. The certification states that information on the application is public information subject to complete disclosure. The public disclosure of the home address and automobile identifying information for agency personnel is unusual. The disclosure of home address and vehicle information would not be routinely required under the Freedom of Information Act. If disclosures are made to assist in finding additional members for a carpool (from within or without the agency), that would not be the same as a public disclosure. Also, depending on how the search for other riders is conducted, general disclosure of home addresses might be avoided if matching is conducted by a third party.

Regardless, once a system of records is established for parking applications, the system notice will have to include a routine use covering those disclosures that are actually made. If the records are, in fact, disclosable publicly, it would be *necessary* to define such a routine use in order to lawfully make the disclosure and to include that information in the Privacy Act notice on the application form. However, unless there is a specific law or policy that mandates these disclosures, the form itself might be revised and the disclosure note removed or revised to reflect actual practice and policy.

46. 5 U.S.C. §552a(u) (1994).

47. Id. at §552a(o).

48. The Directive defining the mission and functions of the Director of the Office of Personnel provides that the Director "serves as the Privacy Act Officer." No specific duties are identified for this responsibility. USITC Directive 1023.1 (2/27/93). Nothing in the Act or in OMB guidance defines the responsibilities of an agency Privacy Act officer or requires that an agency have a Privacy Act Officer.

49. 5 U.S.C. §552a(I)(2) (1994).

50. Id. at §552a(g).

51. Id. at §552a(g)(1)(D).

52. Id. at §552a(b)(11).

53. See *Doe v. Stephens*, 851 F.2d 1457 (D.C. Cir. 1988).

54. "To opposing counsel, a court magistrate or administrative tribunal in the course of a legal proceeding, and to opposing counsel in the course of discovery proceedings for the purpose of enforcing or prosecuting a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issues pursuant thereto."

Appendix

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

September 30, 1996

MEMORANDUM

TO: Inspector General

FROM: Director, Office of Personnel

SUBJECT: Final Response to Inspector General's Draft Report: Analysis of USITC's Privacy Act Systems of Records

I have reviewed the subject report and I find it to be a thorough and thoughtful critique of Privacy Act implementation within the agency. Its major findings , i.e. those relating to the adequacy of existing systems of records and their proper notice -- comport with those identified by agency personnel prior to this audit and the General Counsel had already expended considerable resources in drafting revisions to ITC Systems Notices. Based on discussions with the GC's office, it is my impression that Mr. Gellman's knowledgeable recommendations will be extremely helpful in completing the revisions.

Significantly, the audit report points out that Commission policy has never defined and assigned responsibility for Privacy Act administration. While the Director of Personnel has carried the title of Privacy Act Officer for many years, the report makes clear that no corresponding duties have ever been delineated for such a function and underscores the fact that nothing in the Privacy Act nor OMB guidance defines the responsibilities of a Privacy Act Officer or requires that an agency have one. So far as I am aware, the only articulated responsibilities regarding the Act, which are found in 19 CFR Part 201, subpart D, are

disclosure duties assigned to the Director of Personnel, not to the Privacy Act Officer. In fact, it appears that the limited disclosure responsibility originally assigned to the Director of Personnel led to a later designation as Privacy Act Officer, notwithstanding that the term is without content in Commission policy or directives.

With regard to the far more important aspects of privacy administration such as the identification and publication of systems of records, no Commission policy has ever existed, nor have such responsibilities ever been assigned. However, a great deal of very important work has already been accomplished on this front and is currently ongoing. I am informed by the General Counsel's Office that the redraft of the Commission's systems of records and proposed revision of the Commission's Privacy Act rules is in an advanced stage. I think that Office is to be commended for voluntarily responding to a need which is simply confirmed by this study.

The OGC's work will in fact accomplish the majority of needed actions identified in the report. However, there will still be a need for someone to implement those recommendations of a more administrative nature.

Both the IG and Mr. Gellman, author of the study, admit that there is no "natural fit" for Privacy Act responsibilities in small agencies, where they are generally assigned as collateral duties. Mr. Gellman commented, for instance, that FOIA and Privacy are often combined in such environments and the IG acknowledged that there is a legitimate issue of where Privacy Act responsibilities should be lodged in the Commission. However, in order to avoid any delay in implementing the study's recommendations, she recommends assigning audit implementation to the Director of Personnel, in effect tabling what is the threshold issue of deciding who should be the Privacy Act Officer. The urgency of this matter should be carefully evaluated. First, the report makes quite evident that the agency has little serious vulnerability in this matter. Secondly, the GC's office is already addressing the most important recommendations, thereby reducing further the possibility that needed action will languish.

Finally, whoever is eventually charged with administrative responsibility will need the benefit of participating in this program's implementation, since it will constitute the most substantive experience anyone assigned to it will probably ever receive, although the designee will also need formal training to accomplish effective implementation. Consequently, it seems prudent to avoid letting a somewhat questionable urgency override careful deliberation about what is, in effect, an important issue of resource allocation.

Therefore, I recommend that the Chairman review and determine, as a matter of effective personnel resource allocation, where Privacy Act administration should be assigned. This would be simultaneous with the GC effort to complete the important work already in progress, which will in fact form the fundamental framework for successful Privacy Act administration. I am happy to assist in this review and to participate in any capacity, either as individual adviser or in some joint evaluative process as designated by the Chairman.

This response and the recommendation contained herein were approved by the Chairman on this date.

cc: The Commission
General Counsel
Acting Director, Office of Administration