Document Revision History for: _____

Version	Date	Author	Change Description

SECTION 10 PRIVACY ACT REQUIREMENTS

10.1 Purpose

10.1.1 The purpose of this section is to provide guidance to the Maritime Administration (MARAD) project managers about the responsibilities imposed by the Privacy Act 1974, as amended by The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. 552a).

10.2 Scope

The provisions of this policy apply to all MARAD IT Projects which maintain, collect, use, or disseminate information subject to the Privacy Act of 1974, as amended.

10.2.1 The Privacy Act of 1974, as amended, applies to “system of records”. The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

The Privacy Act requires each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, and shall**:**

10.2.1.1 Establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains personally identifiable information (PII) records pertaining to him;

10.2.1.2 Define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

10.2.1.3 Establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

10.2.1.4 Establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

10.2.1.5 Establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

10.3 References

10.3.1 5 U.S.C. 552a, The Privacy Act of 1974, as amended by The Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503)

10.3.2 Privacy Act Implementation, Guidelines and Responsibilities (FR; July 9, 1975)

10.3.3 The Privacy Act of 1974; Final Guidance (FR; June 19, 1989), Interpreting the Provisions of The Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503)

10.3.4 The Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974 (FR; April 23, 1991)

10.3.5 OMB, Circular A-130, Management of Federal Information Resources, dated November 30, 2000

10.3.6 OMB, Guidance on Inter Agency Sharing of Personal Data Protecting Personal Privacy, M-01-05, dated December 20, 2000

10.3.7 DOT Privacy Act Issuances (65 FR 19475; April 11, 2000) DOT's Guide for FOIA or Privacy Act Requesters

10.3.8 Children's Online Privacy Protection Act (COPPA) of 1998, Title XXXIII.

10.4 Applicability

This section applies to MARAD administration records maintained in systems known as a "system of records." A "system of records" may include paper and/or automated records that maintain, collect, use, or disseminate information subject to the Privacy Act of 1974, as amended.

10.5 Definitions

See Appendix 10-1 to this section.

10.6 Responsibilities

10.6.1 The MARAD CIO is responsible for:

10.6.1.1 Providing guidance to MARAD managers, supervisors and employees concerning the implementation and application of the Privacy Act, as amended; and

10.6.1.2 Designating an individual as the MARAD Privacy Act Officer.

10.6.2 The MARAD Privacy Act Officer is responsible for:

10.6.2.1 Establishing procedures for individuals to gain access to information on them that are in a system of records which have been changed (includes an amendment or correction of records);

10.6.2.2 Ensuring preparation and publishing of a System of Records Notice (SORN), which is a public notice in the Federal Register of the establishment, or revision, of a system of records;

10.6.2.3 Evaluating the effectiveness of MARAD's compliance with the Privacy Act, as amended;

10.6.2.4 Reviewing each ongoing matching program in which MARAD has participated to ensure that all requirements have been met;

10.6.2.5 Justifying any disclosures under subsection (b) of the Privacy Act, which provides exceptions to the Act's prohibition on disclosure;

10.6.2.6 Giving notice in writing to individuals in accordance with subsection (e)(3) of the Privacy Act;

10.6.2.7 Providing guidance to Project Managers on their responsibilities;

10.6.2.8 Preparing, executing, and monitoring matching agreements, following the guidelines as outlined in The Computer Matching and Privacy Protection Amendments of 1990; and

10.6.2.9 Securing approval of the DOT Data Integrity Board (DIB), as required, for all computerized matches of automated Privacy Act systems of records whether covered by the Privacy Act or not.

10.6.3 Project/System Managers are responsible for:

10.6.3.1 Establishing policies and practices for their system(s) of records;

10.6.3.2 Safeguarding the security of the system(s) they manage in order to prevent unauthorized disclosures;

10.6.3.3 Immediately advising MARAD's Freedom of Information Act (FOIA) Officer whenever a request for access or amendment of a system of records is received;

10.6.3.4 Completing a PIA and/or SORN, if required; and

10.6.3.5 Ensuring that no official files are maintained which are retrievable by name or other identifier unless a SORN has been published in the Federal Register;

10.6.4 Each system user/operator is responsible for: Ensuring that no record contained in a system of records is disclosed to any person or entity outside MARAD without prior written consent of the individual who is the subject of the record. However, disclosure may be made to people within MARAD and to entities outside MARAD without the prior consent of the individual when one or more of the exceptions to this prohibition discussed in 5 U.S.C. §552a-part (b) of the Privacy Act, as amended "Conditions of Disclosure" apply. All requests for information subject to the Privacy Act must be coordinated through the MARAD Privacy Act Officer.

10.7 Task and Activities

10.7.1 PIA Preparation. Not every project will require a PIA. No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged (See Appendix 10-2). The Project Manager shall complete the initial steps of the PIA Requirement Determination form, Appendix 10-2, to document that a PIA is or is not required.

10.7.2 PIA preparation is required when:

10.7.2.1 A project or system creates any new collections of personal information; or

10.7.2.2 A new technology or system is developed or procured that stores personal information; or

10.7.2.3 A project or system collects or combines PII on individuals electronically that can be used to identify them particularly; or

10.7.2.4 One collection (project or system) may not reveal a person's identity, but if it is technologically possible to combine data by using a business intelligence tool so as to reveal the true identity of some individual;

10.7.2.5 Altering an existing database or systems in order to incorporate PII; or

10.7.2.6 Creating new databases or views from old databases or systems which contain personally identifying information. Changes are often made to make data access more user-friendly and effective, and often are done by special request and never get attention beyond the fix or change. A PIA must be completed to demonstrate that data access and Privacy were considered when the changes were made.

10.7.3 PIAs in the SDLC process

10.7.3.1 PIAs should be completed early in the SDLC process for a new system. A PIA must be completed prior to KDP 1, Project Authorization.

10.7.3.2 PIAs must be completed prior to pilots or test projects.

10.7.3.3 PIAs must be completed on all systems whether they reach the budget level of an OMB-300 or not, e.g. OMB-53.

10.8 Artifacts

10.8.1 Privacy Act Risk Assessment. Privacy Act Risk Assessments will be completed at the direction of the Decision Authority. The Risk Assessment will review all requirements of the Privacy Act, list any findings, and provide recommendations for resolving findings, if identified. Privacy Act Risk Assessment Templates are contained in Appendix 10-3, Privacy Risk Assessment, Privacy Act of 1974 (5 U.S.C. 552a) and Appendix10- 4, E-Government Act of 2002: Section 208 Privacy Provisions (H.R>2458). If information on children under 13 years of age is being collected the Project Manager must consult the Privacy Officer to ensure requirements of the Children's Online Privacy Protection Act (COPPA) are met.

10.8.2 Privacy Impact Assessment (PIA). The PIA will document, at the early stage of a project, how the new or revised IT system will have privacy built into the fundamental architecture of the system, including technology choices. The length and coverage of a PIA will vary by the size and complexity of the IT project. A PIA Template is contained in Appendix 10-5 of this section.

10.8.3 System of Records Notice (SORN). Notice filed in the Federal Register for new systems or modifications to systems that identify and categorize the information that the systems will handle. Format for SORN is contained in Appendix 10-6.

10.9 Issues and Concerns

PIAs are not required for all systems. Project Managers must ensure that an initial analysis is performed to determine if a PIA is required. A PIA Requirement Determination, Appendix 10-2, shall be completed and approved for all systems.

10.10 Review Activity

The Project Manager or designated expert will prepare the PIA. The MARAD Privacy Officer will work with the Project Manager to finalize the PIA content and format. The PIA will be approved by the MARAD Privacy Officer prior to forwarding to the DOT Privacy Officer for approval.

APPENDIX 10-1

Definitions

1. Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.

2. Maintain. Includes keeping, collecting, using or disseminating information.

3. Matching Program.

3.1 Any computerized comparison of –

3.1.1 Two or more automated systems of records or a system of records with non-Federal records for the purpose of-- (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or (II) recouping payments or delinquent debts under such Federal benefit programs, or

3.1.2 Two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

3.2 Does not include –

3.2.1 Matches performed to produce aggregate statistical data without any personal identifiers;

3.2.2 Matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

3.2.3 Matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;

3.2.4 Matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

3.2.5 Matches--(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or (II) conducted by an agency using only records from systems of records maintained by that agency; if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

3.2.6 Matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or

3.2.7 Matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1).

4. **Personally Identifiable Information (PII):** Information relating to an individual which discloses the identity of such individual.

5. Privacy Impact Assessment (PIA). A process used to evaluate the collection of personal data in information systems. The objective of a PIA is to determine if collected personal information data is necessary and relevant. To accomplish this objective, a PIA is used to identify and address information privacy when planning, developing, implementing, and operating individual agency information management systems and integrated information systems. A PIA will assess "*security and privacy risks*" associated with operating information systems that collect, access, use, or disseminate personal information.

6. Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

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

8. Statistical Record. A record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of Title 13.

9. **System of Records.** A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

APPENDIX 10-2 PIA REQUIREMENT DETERMINATION

Check List

System Name: **System Number:**	
Major: ☐ **Non Major:** ☐	
CONTACT INFORMATION	
Main Contact Name:	
Email Address: **Office Room Number:** **Phone Number :**	
SYSTEM INFORMATION	
1. Does/will this system contain Personally Identifiable Information (PII) for 10 or more people in either of the following categories?: • **Public, consumers, citizens** • **State/local government employees or contractors** (Note: federal government employees/contractors do NOT fall within the above categories)	**Yes** ☐ ***** No ☐
2. Is this a new system, or are there changes to an existing system?	**New** ☐ ***** Change ☐ No Changes ☐
3. If there are changes to an existing system, do any of these changes affect how PII is collected, used, shared, handled, stored, or accessed?	**Yes** ☐ ***** No ☐ N/A ☐
Please describe the types of information that this system involves.	
What changes are planned, if any?	

NOTES: PIA Required? (see footnote and circle response) **YES** ☐ **NO** ☐

Prepared by: _____ Approved by: _____

MARAD Project Manager MARAD Privacy Officer

If "Yes" to question 1 and 3, a PIA IS required. If "Yes" to question 1, and if a New system, a PIA IS required.

MA-1037A (E) (12/05)

APPENDIX 10-3

Privacy Risk Assessment
Check List

INSERT SYSTEM NAME

Privacy Act of 1974 (5 U.S.C. 552a)

The requirements of The Privacy Act apply only to "systems of records." Under the law, a "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *See 5 U.S.C. 552a (a)(5).* The following table details the most important requirements that agencies must follow to comply with the Privacy Act.

REQUIREMENT	FINDINGS	RECOMMENDATION
Each agency that maintains a system of records shall: Publish in the Federal Register a Privacy Act Notice when a system of records is established or revised that details the existence and character of the system and includes: o The name and location of the system; o The categories of individuals on whom records are maintained in the system; o The categories of records maintained in the system; o Each routine use of the records contained in the system, including categories of users and the purpose of such use; o The policies and practices of the agency regarding storage, retrievability, access controls, retention and disposal of records; o The title and business address of the agency official who is responsible for the system of records; o The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; o The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; o The agency procedures whereby an individual can be notified at his/her request how he/she can gain access to any records pertaining to him/her contained in the system of records and how he/she can review the contents; and o The categories of sources of records in the system. *See 5 U.S>C. 552a(e)(4).* o For an existing system of records, at least 30 days prior to publication of the Privacy Act Notice, publish in the Federal Register notice of any new use or intended use of the information in the system and provide an		

REQUIREMENT	FINDINGS	RECOMMENDATION
opportunity for interested persons to submit written comment to the agency. See 5 U.S.C. 552a(e) (11).		
Inform each individual whom it asks to supply information, either on the form where it asks for the information or on a separate form that can be retained by an individual: 1) the authority under which the agency is seeking the information and whether the disclosure is mandatory or voluntary; 2) the principal purpose or purposes for which the information is intended to be used; 3) the routine uses which may be made of the information; and 4) the effects on an individual if he or she chooses to not provide the information. See 5 U.S.C. 552a(e)(3).		
Maintain in its records only information about individuals that is relevant and necessary to accomplish an agency's purpose. See 5 U.S.C. 552a(e)(1).		
Collect information to the greatest extent practical directly from an individual when the information may result in adverse determinations about an individual's rights. See 5 U.S.C. 552a(e)(2).		
Maintain all records with accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to an individual. See 5 U.S.C. 552a(e)(5).		
Establish and conduct training on rules of conduct for persons involved in the design, development, operation or maintenance of any system of records, including training on penalties for noncompliance. See 5 U.S.C. 552a(e)(9).		
Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats of hazards to their security which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. See 5U.S.C 552 a (e)(10).		
Access: Upon request, provide an individual with access to his or her record and allow the record to be reviewed and a copy made; permit the individual to request amendment of the records if disagreement occurs; establish fees to be charged, if any, to any individual for making copies of his or her record. See 5 U.S.C. 552a(d).		

APPENDIX 10-4

E-Government Act of 2002:

Section 208 Privacy Provisions (H.R.2458)

Risk Assessment
Check List
INSERT SYSTEM NAME

The E-Government Act of 2002 outlines substantial privacy provisions for federal agencies in Section 208. The law requires the Office of Management and Budget (OMB) to provide guidance to agencies on complying with Section 208. The following information details such guidance.

REQUIREMENT	FINDINGS	RECOMMENDATION
Federal agencies must conduct Privacy Impact Assessments (PIAs) for electronic information systems and collections: o In general, agencies must perform and update PIAs as necessary where a system change creates new privacy risks. Specifically, agencies must conduct PIAs: 1) prior to developing and procuring IT systems or projects that collect, maintain or disseminate information in identifiable form or about members of the public, or 2) prior to initiating a new electronic collection of information in identifiable form for 10 or more persons. o No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged.		
The depth and content of PIAs should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.		
Agencies must ensure that the PIA document is approved by a "reviewing official."		
The PIA must be submitted to OMB.		

REQUIREMENT	FINDINGS	RECOMMENDATION
The PIA document must be made publicly available.		
Federal agencies must post privacy policies on agency Web sites used by the public.		
Privacy policies must: o Address the nature, purpose, use and sharing of information collected; o Inform visitors whenever providing requested information is voluntary; o Inform visitors how to grant consent for use of information; o Notify Web visitors of their Privacy Act Rights: in the body of the privacy policy; via link to the applicable agency regulation; or via link to other official summary of statutory rights; o Specify what information the agency collects automatically (e.g. IP address, time of visit, etc), and identify the use for which it is collected; o Comply with COPPA, if agency practices make such relevant; o In clear language, include information about management, operational and technical controls ensuring the security and confidentiality of personal information; and information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems; o Be posted on agencies' principal Web sites; on any known, major entry points to agency Web sites; and on any Web page that collects substantial information in identifiable form; o Be: clearly labeled and easily accessed; written in plain language; and made clear and easy to understand (e.g. "short/layered notices").		
Federal agency Web sites: o Are prohibited from using persistent cookies or any other means to track		

REQUIREMENT	FINDINGS	RECOMMENDATION
visitors' activity, except: o Agency heads may approve the use of persistent cookies for a compelling need. In such a case, the agency's privacy policy must include: 1) the nature of the information collected; 2) the purpose and the use of the information; 3) whether and to whom the information will be disclosed; and 4) the privacy safeguards applied to the information collected. o Are allowed to use session cookies and other technology that does not persist over time.		
Federal agencies must translate privacy policies into a standardized machine-readable format that alerts users automatically about whether site privacy practices match their personal privacy preferences.		

MA-1037C (E) (12/05)

APPENDIX 10-5

PRIVACY IMPACT ASSESSMENT
Check List

<System Name>

System Name:	**System Identifier:**
Preparer:	**Office:**
Date:	**Phone:**

This project is in the following stage(s): Use the MARAD SDLC ITAM Section 4 as guidance. Initial (Initiation Phase); Planning (Planning Phase); Full Acquisition (Requirements Definition, Design, Development, Test, Implementation); Steady State (Operations & Maintenance); Mixed Life Cycle (Combination of the aforementioned Phase)

Initial ☐ Planning ☐ Developmnet, Modernization & Enhancement ☐ Steady State ☐ Mixed Life Cycle ☐

I. Data in the System

1. Generally describe what information will be collected in the system.
2. What are the sources and types of the information in the system?
3. How will the data be used by MARAD?
4. Why is the information being collected? (Purpose)

II. Access to the Data

1. Who will have access to the data in the system (*internal and external parties*)? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (*24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act*)?

2. What controls are in place to prevent the misuse of data by those having authorized access?

3. Do other systems share data or have access to data in this system? If yes, explain who will be responsible for protecting the privacy rights of the individuals affected by the interface? (i.e., *System Administrators, System Developers, System Managers*)

4. Will other agencies, state or local governments share data or have access to data in this system?

5. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? If yes, how is notice given to the individual? (*Privacy policies must clearly explain where the collection or sharing of certain information may be optional and provide users a mechanism to assert any preference to withhold information or prohibit secondary use.*)

APPENDIX 10-5 (Continued)

PRIVACY IMPACT ASSESSMENT
Check List

<System Name>

Submitted by: _____
Project Manager

MARAD Approval: _____
MARAD Privacy Officer

DOT Approval: _____
DOT Privacy Officer

MA-1037D (E) (12/05)

APPENDIX 10-6

GUIDELINES FOR ESTABLISHING A NEW PRIVACY ACT SYSTEM OF RECORDS NOTICE

All Privacy Act system of records notice actions are transmitted electronically to MARAD Privacy Officer for forwarding to the DOT Privacy Officer.

It takes approximately 120 days to establish a new system, which includes the required approval by DOT and Congress and publication in the Federal Register.

The format for systems of records notice is as follows:

SYSTEM IDENTIFICATION:

SYSTEM NAME: The system name should indicate the general nature of the system of records and, if possible, the general category of the individual to whom it pertains. It may not exceed 55 character positions, which includes punctuation and spaces. Acronyms are discouraged unless there is room to spell them out completely.

SYSTEM LOCATION:

a. For a system maintained in a single location, provide the official organizational name and complete mailing address, using the postal service's two letter state abbreviation and nine-digit zip code.

b. For a geographically or organizationally decentralized system, list addresses for all activities that maintain a portion of the system of records.

c. For an automated data system with a central computer facility and input or output terminals at geographically separate locations, list complete mailing addresses for each location.

d. If multiple locations are identified, the system location may indicate that the official mailing addresses are contained in the MARAD or Department Directory.

e. Do not use classified addresses. If necessary, state that the addresses are classified.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Identify the individuals for whom records are being collected.

CATEGORIES OF RECORDS IN THE SYSTEM: Describe in clear, non technical terms the types of records maintained in the system. Limit the description to documents actually retained in the system of records. Do not describe source documents that are used only to collect data and then destroyed. Remember to include each item of information that will be identified in the "Retrievability" paragraph discussed below. For example, if you are retrieving information based on an individual’s social security number, include this item in this category.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: List the federal laws, executive orders, etc., that allow you to collect and maintain the information. The authorities are in numeric order beginning with the laws and followed by the Executive Orders. The basic statute we use for general collection is 5 U.S.C. 301, Departmental Regulations and if we are collecting the SSN, we cite to E.O. 9397.

PURPOSE: List the specific purpose(s) for which the system of records is maintained, ensuring that you cite the uses for the records within the activity and the rest of the DOT.

ROUTINE USES:

At the beginning of the entry, state: "In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the MARAD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:"

Then, list all disclosures of the records outside the MARAD/DOT, including the recipient of the disclosed information and the uses the recipient will make of it. For example, "To state and local agencies in the performance of their official duties related to verification of status for determination of eligibility for Veterans Bonuses and other benefits and entitlements, including Department of Labor and state unemployment agencies for unemployment compensation for ex-service members."

Do not use general statements such as "to other Federal Agencies as required."

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS:

STORAGE: State the method(s) used to store the information in the system. For example: Automated and manual records; computerized data base; microform.

RETRIEVABILITY: Indicate how records are retrieved. For example, "Name and Social Security Number." [Note: this information should be included under "Categories of Records in the System."

SAFEGUARDS: Generally identify the methods used to protect the records from unauthorized disclosure or tampering. But, do not describe the safeguards in such detail as to compromise system security.

An example is "Computer facilities and terminals are located in restricted areas accessible only to authorized persons that are properly screened, cleared and trained. Information is password protected. Manual records and computer printouts are available only to authorized personnel having a need-to-know."

SYSTEM MANAGER (S) AND ADDRESS(ES): Provide the organization title and a complete mailing address of the activity responsible for maintaining the system. If the record holder is different than the policy official, then list both.

NOTIFICATION PROCEDURE:

This describes how the individual can determine if a record in the system pertains to him/her. Standard language is as follows: "Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to [Note: list title and mailing address of activity holding the records].

The request should be signed and include [insert items of information listed under the Retrievability paragraph above (i.e., dates of service, social security number, etc) and a complete mailing address.

RECORD ACCESS PROCEDURE:

This describes how an individual can review the record and obtain a copy of it. Standard language is as follows: "Individuals seeking access to records about themselves contained in this system of records should address written inquiries to [Note: list title and mailing address of activity holding the records]. The request should be signed and include [insert items of information listed under the Retreivability paragraph above (i.e., dates of service, social security number, etc) and a complete mailing address.

CONTESTING RECORD PROCEDURE: The standard caption reads: "State where the rules for accessing records, and for contesting contents and appealing initial agency determinations are published or may be obtained from the system manager."

RECORD SOURCE CATEGORIES: This caption describes who, where, or what the information is usually taken from.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

If no exemption has been established for the system, indicate "None." If an exemption has been established, then cite the exemption. For example: "Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principal function any activity pertaining to the enforcement of criminal laws.

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b) (1), (2), and (3), (c) and (e) and published in 32 CFR part 701, subpart G. For additional information contact the system manager."