invasion of privacy. Unsupported assertions will not meet this burden. In the absence of exceptional, documentable circumstances, this information will be released. We will always make submissions from organizations or businesses, or from individuals identifying themselves as representatives or officials of organizations or businesses, available for public inspection in their entirety. If you wish to review a copy of the Regional Plans, please contact Ms. Laurie Sharp to find the office nearest you.

Dated: May 9, 2007.

Richard J. Woodley,

Regional Resources Manager, Mid-Pacific Region, Bureau of Reclamation.

[FR Doc. E7–11689 Filed 6–15–07; 8:45 am]

BILLING CODE 4310–MN–P

DEPARTMENT OF JUSTICE

[AAG/A Order No. 019–2007]

Privacy Act of 1974; Systems of Records

AGENCY: United States Marshals Service, Department of Justice.

ACTION: Notice of modified systems of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974 (5 U.S.C. 552a), the United States Marshals Service (USMS), Department of Justice, is issuing public notice of its proposal to modify its systems of records. This notice publishes updates to those systems of records, last published in the **Federal Register** on November 8, 1999 (64 FR 60832–52), except as otherwise set forth below under the caption **SUPPLEMENTARY INFORMATION**.

DATES: Title 5 U.S.C. 552a(e)(4) and (11) provide that the public be given a 30-day period in which to comment on routine uses. The Office of Management and Budget (OMB), which has oversight responsibility under the Act, requires a 40-day period in which to review the systems modifications. The public, OMB and Congress are invited to comment on the modifications to these systems. Please submit any comments by July 30, 2007. The proposed changes will be effective on that date, unless comments are received that result in a contrary determination.

ADDRESSES: Submit written comments to the Department of Justice (DOJ), ATTN: Mary E. Cahill, Management and Planning Staff, Justice Management Division, Washington, DC 20530 (Room 1400, NPB), facsimile number 202–307–1853.

FOR FURTHER INFORMATION CONTACT: Ed Bordley, Attorney-Advisor, USMS, at 202–307–8571.

SUPPLEMENTARY INFORMATION: Modifications to the USMS systems of records include: Updates to addresses for the systems locations and systems managers' locations; corrections to office designations for systems locations and titles of systems managers; revisions to reduce redundancy and increase clarity; additions or changes to more accurately describe the systems' categories of individuals, purposes, categories of records and record source categories; clarifications to existing routine uses; additions to the routine uses; updates to the retention and disposal sections; and additions to data elements omitted from previous notices. Specific changes for each USMS system of records notice are set forth below:

USMS Badge & Credentials File, Justice/USM–001: The system location and system manager location address have been updated. The section on categories of individuals covered by the system has been changed. Routine uses have been added and the others revised. An element has been added under storage. Under record source categories, the category ''individuals for whom the badges/credentials were made'' was added.

USMS Internal Affairs System, Justice/USM–002: The system location and system manager location address have been updated; the system manager's designation has also been changed. The record categories designation was modified to reflect the change in the system manager's designation. The categories of individuals and record source categories were expanded to be more specific. Routine uses have been added and the others revised.

Special Deputation Files, Justice/USM–004: The system location and system manager location address has been updated; the system manager's designation has also been changed. The categories of individuals covered designation has been expanded to be more specific. Minor revisions were made to the categories of records. Routine uses have been added and the others revised. The record source categories subdivision has been revised to include individual applicants.

USMS Prisoner Processing and Population Management/Prisoner Tracking System (PPM/PTS), Justice/USM–005, last published in the ***Federal Register*** *on April 28, 2004 (69 FR 23213):* The system manager designation has been changed. New categories have been added to the categories of individuals covered. Under routine uses, the markers have been changed from numeric to alpha characters to match the other system notices. Three routine uses were removed to eliminate redundancy; and one was added. The record source categories designation was revised to reflect the changes in the individual categories.

USMS Training Files, Justice/USM–006: The primary system location and system manager location address have been updated. The wording has been changed for the categories of individuals covered. Routine uses have been added and minor revisions made to others. The retention and disposal period has been corrected.

Witness Security Files Information System, Justice/USM–008: The system location and system manager location address have been updated. The section on categories of individuals covered has been expanded to include potential witnesses and witnesses' or potential witnesses' families; the wording has also been changed. The categories of records has been revised to reflect the changes made in the categories of individuals. Routine uses have been added and one routine use has been removed. The retention and disposal category has been corrected; the record source categories have also been modified.

Inappropriate Communications/Threat Information System (IC/TIS), Justice/USM–009: The primary system location and system manager location address have been updated. Routine uses were added and minor revisions made to the others. The retention and disposal category has been corrected. The record source categories have been revised to include the threat or inappropriate communication initiator.

Judicial Facility Security Index System, Justice/USM–010: The system location and system manager location address have been updated. ''USMS facilities'' has been added to the categories of individuals covered. Routine uses were added and minor revisions made to the others. ''Contractor'' has been added to the retrievability category.

Judicial Protection Information System, Justice/USM–011: The system location and system manager location address have been updated. A ''Decentralized Segment'' has also been added under system location. Routine uses have been added and minor revisions made to the others. The record source category has been reworded.

U. S. Marshals Service Administrative Proceedings, Claims, and Civil Litigation Files, Justice/USM–013: The system location and system manager location

address have been updated. Routine use (f) was reworded. Routine uses were added and minor revisions made to the others.

USMS Key Control Record System, Justice/USM–016: The system location address has been updated and a decentralized location added. The system manager has also been changed. The categories of individuals covered was modified to reflect the decentralized location change. The record categories designation was changed to eliminate redundancy. Routine uses were added and minor revisions made to others.

Judicial Security Staff Inventory System, USMS–017: The system location and system manager location address have been updated. The categories of individuals covered has been expanded to include contract employees and other individuals. Routine uses have been added and minor revisions made to the others.

USMS Alternative Dispute Resolution (ADR) Files and Database Tracking System, USM–018: The system location and system manager location address have been updated. Routine uses have been added and minor revisions made to the others.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report on the modified systems to OMB and the Congress. Descriptions of these systems are found below.

Dated: June 5, 2007.

Lee J. Lofthus,

Assistant Attorney General for Administration.

JUSTICE/USM–001

SYSTEM NAME:

U.S. Marshals Service Badge & Credentials File.

SECURITY CLASSIFICATION:

Limited official use.

SYSTEM LOCATION:

Human Resources Division, United States Marshals Service, CS–3, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former U.S. Marshals Service (USMS) personnel, other federal employees, and student volunteers or other workers when they are performing work for the USMS.

CATEGORIES OF RECORDS IN THE SYSTEM:

Personnel data system established to control issuance of badges and credentials to USMS personnel which contains photographs of all employees and hand receipts showing the employee's name, title, duty location, badge and credential numbers, and date of issuance.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and 44 U.S.C. 3101.

PURPOSE(S):

The Badge & Credentials File system assists in controlling the issuance of badges and credentials to USMS personnel which are used for identification purposes in the performance of official duties.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

This file serves as a record of issuance of credentials. Information from this file may be disclosed:

(a) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records;

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(h) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(i) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

(j) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Records are kept in standard folders and kept electronically.

RETRIEVABILITY:

Records are indexed and retrieved by the individual's name and numerical order of badges and credentials.

SAFEGUARDS:

Access is restricted to personnel of the Background and Suitability Team, Human Resources Division. Records are maintained in metal filing cabinets which are locked during non-duty hours.

RETENTION AND DISPOSAL:

Records are kept for duration of employee's tenure in the service. Records are destroyed when superseded or obsolete.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Human Resources Division, United States Marshals Service, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as ''Record access procedures.''

RECORD ACCESS PROCEDURES:

A request for access to a record from this system shall be made in writing with the envelope and the letter clearly marked ''Privacy Act Request.'' It should clearly indicate the name of requester, the nature of the record sought and the approximate dates covered by the record. The requester shall also provide the required verification of identity (28 CFR 16.41(d)) and provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above, Attention: FOI/PA Officer.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the address of the System Manager listed above, Attention: FOI/PA Officer, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Record of Notification of Employment by U.S. Marshals Service, Human Resources Division and the individuals for whom the badges/credentials are made.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/USM–002

SYSTEM NAME:

Internal Affairs System.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

United States Marshals Service (USMS), Operations Support Division, CS–3, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

USMS employees reported for or investigated for alleged misconduct.

CATEGORIES OF RECORDS IN THE SYSTEM:

The Internal Affairs System contains statements of the investigator and witnesses, exhibits and reports of investigations prepared by the Office of Inspection, USMS, on findings of alleged misconduct of USMS employees, and records on the disposition of the investigation.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 509 and 510; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111(n).

PURPOSE(S):

The Internal Affairs system is maintained in order to carry out the responsibility of investigating allegations of improper conduct on the part of USMS employees, and to support adverse personnel actions and proceedings which may result based on the findings of the investigation.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

RECORDS OR INFORMATION MAY BE DISCLOSED:

(a) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim;

(b) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(c) To any person or entity that the USMS Office of Internal Investigations has reason to believe possesses information regarding a matter within the jurisdiction of the USMS Office of Internal Investigations, to the extent deemed to be necessary by the Office in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity;

(d) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(e) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(f) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(g) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(h) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(i) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(j) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires

information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Originals stored in standard file folders. Duplicate copies are maintained on compact discs.

RETRIEVABILITY:

Information is retrieved by the employee's name and case file number.

SAFEGUARDS:

Records are stored in locked safe. Access to automated records is protected by user identification and passwords.

RETENTION AND DISPOSAL:

Records are transferred to the Washington National Records Center three years after the case or investigation is closed, and destroyed 10 years after the close of the case or investigation.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Office of Inspection, Operations Support Division, U.S. Marshals Service, CS–3, Washington DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as the ''Records access procedures.''

RECORD ACCESS PROCEDURES:

To the extent that this system is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked ''Privacy Act Request.'' It should clearly indicate name of the requester, the nature of the record sought and approximate dates covered by the record. The requester shall also provide the required verification of identity (28 CFR 16.41(d)) and provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above, Attention: FOI/PA Officer.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager identified above, stating clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Sources of information contained in this system are the individuals covered by the system, individuals and entities contacted by investigators, and government records.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4)(d), (e)(1), (2), and (3), (e)(4)(G) and (H), (e)(5), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2) and (k)(5). To the extent that investigations reveal actual or potential criminal or civil violations, this system is additionally exempt from subsection (e)(8) of the Privacy Act pursuant to 5 U.S.C. 552(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the **Federal Register**. See 28 CFR 16.101.

JUSTICE/USM–004

SYSTEM NAME:

Special Deputation Files.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

United States Marshals Service (USMS), Investigative Services Division, CS–4, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Federal, state and local law enforcement employees; physical security and personal protection employees; USMS employees; and USMS contract personnel appointed to perform the functions of Deputy U.S. Marshals.

CATEGORIES OF RECORDS IN THE SYSTEM:

Special Deputation files contain agency request letters, individual applications for special deputation, notifications to local U.S. Marshal to swear in special deputies, copies of oath of office and credentials of persons utilized as deputy marshals.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 CFR subpart T, 0.112, 28 U.S.C. 562.

PURPOSE(S):

The USMS is authorized to deputize selected persons to perform the functions of a Deputy U.S. Marshal whenever the law enforcement needs of the USMS so require, to provide courtroom security for the Federal judiciary, and as designated by the Associate Attorney General pursuant to 28 CFR 0.19(a)(3). USMS Special Deputation files serve as a centralized record of the special deputations granted by the USMS to assist in tracking, controlling and monitoring the Special Deputation Program. Routine uses of records maintained in the system, including categories of users and the purposes of such uses: Records or information may be disclosed:

(a) To a federal, state or local law enforcement agency regarding that agency's USMS deputized employees;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(d) To the news media and the public, including disclosures pursuant to 28

CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(h) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(i) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(j) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel—related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Records are filed in standard file cabinets. Duplicate copies of paper records are stored on magnetic discs.

RETRIEVABILITY:

Files are indexed by name and by government department.

SAFEGUARDS:

Records are kept in a locked file. Computerized records are password protected.

RETENTION AND DISPOSAL:

Records are cut off annually upon expiration and destroyed when they are five years old.

SYSTEM MANAGER(S) AND ADDRESS:

Chief of Special Deputation Unit, Investigative Services Division, U.S. Marshals Service, CS–4, Washington, DC 20530–1000.

NOTIFICATION PROCEDURES:

Same as the ''Records access procedures.''

RECORDS ACCESS PROCEDURES:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly, marked ''Privacy Act Request.'' It should clearly indicate name of the requester, the nature of the record sought and approximate dates covered by the record. The requester shall also provide the required verification of identity (28 CFR 16.41(d)) and provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above, Attention: FOI/PA Officer.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager identified above, stating clearly and concisely what information is being contested, the reasons for contesting it and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Information is derived from individual applicants and agencies requesting special deputations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/USM–005

SYSTEM NAME:

U.S. Marshals Service Prisoner Processing and Population Management/Prisoner Tracking System (PPM/PTS).

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Primary System: Witness Security and Prisoner Operations, U.S. Marshals Service, 11th Floor, CS–4, Washington, DC 20530–1000.

Decentralized Segments: Each district office of the U.S. Marshals Service (USMS) maintains only files on prisoners taken into custody of the U.S. Marshal for the respective district. The addresses of USMS district offices are on the Internet at (*http://www.usmarshals.gov*).

Centralized Segment: The Contractor with whom the USMS has contracted to establish and manage a nationwide integrated health care delivery system and to process and pay medical claims will maintain a single site for appropriate paper documents (e.g., invoices) and automated files online related to these activities (e.g., names and addresses of hospitals, physicians and other health care providers and support service systems).

Medical Records: Records generated by community physicians, hospitals, and ancillary support service systems developed by the Contractor as participants in the Preferred Provider Network (PPN) to deliver health care services for USMS prisoners are maintained by the respective offices of these licensed providers. Addresses of these licensed providers may be obtained by contacting the USMS Office of Interagency Medical Services (OIMS), Prisoner Services Division at the address above.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Arrestees, fugitives, prisoners, and other individuals under custody of the USMS and prisoner health care services providers under the USMS Managed Health Care Contract.

CATEGORIES OF RECORDS IN THE SYSTEM:

Any and all information necessary to complete administrative processes, safekeeping, health care, and disposition of individual Federal prisoners who are in custody pending criminal proceedings, together with any law enforcement related records generated during such custody. Records include a compilation of basic information on each individual taken into the U.S. Marshals Service's custody including identifying data, reason for U.S. Marshal custody (e.g., Federal indictment, complaint, or writ), the court disposition of charges, custody dates, and institutions to which individuals are committed or housed. The records also encompass Form USM–129, Prisoner Custody, Detention and Disposition Record (formerly DJ–100); prisoner photograph; personal history statement; fingerprint card; identification record; detainer notice; speedy trial notice; prisoner remand or order to deliver prisoner, and receipt for U.S. prisoner; property receipt; court records including writs, bail/bond release information, judgment and commitment and other court orders; prisoner alert notice; prisoner complaints or serious incident reports (and related investigatory information) filed by either the prisoner or by officials or by other individuals at the institution where the prisoner is housed and covering a wide range of potentially serious issues, e.g., medical treatment of prisoners, and attempted escapes or alleged prisoner misconduct or criminal activity; designation requests to Bureau of Prisons (BOP) and BOP responses; information identifiable to informants, protected witnesses, and confidential sources; access codes and data entry codes and message routing symbols used to communicate with law enforcement officials regarding the custody and safekeeping of prisoners; and prisoner transportation requests to the Prisoner Transportation Division (and any related records) which may include sensitive security data. Medical records included in this system consist of nurses' notes of medical problems, diagnosis, treatment recommended; names of health care providers at the housing unit, social workers, attorneys, family members and USMS contact personnel; special issue or treatment notices; names and addresses of community treatment facilities, physicians and other community health care providers and support service systems, dates of service, provider tax identification numbers; medical care given, cost of care, and billing records. Medical records generated by health care providers may be included in this system of records, as necessary for continuity of care/appropriate care or infectious disease control.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

18 U.S.C. 3149, 3193, 3604, 3621, 4002, 4006, 4086, 4285; 28 U.S.C. 509, 510, 568, 569; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111.

PURPOSE(S):

The Prisoner Processing and Population Management/Prisoner Tracking System (PPM/PTS) is maintained to cover law enforcement and security related records which are generated in the local USMS district offices in connection with the processing, safekeeping, and disposition of individuals in USMS's custody. Medical records included in this system assist consultation and coordination between the USMS district office, the housing unit, treatment facility, health care provider, transportation facility, and other Federal agencies, e.g., BOP, to ensure that prisoners in custody of the U.S. Marshals are given proper treatment. Through USMS nursing staff, districts are assisted in determining medical treatment necessary while the prisoner is in custody of the U.S. Marshal and in ensuring the prisoner's medical clearance for travel.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Records or information may be disclosed:

(a) To other federal, state, local or foreign law enforcement agencies; contractors and/or subcontractors; contract detention or medical facilities; and health care providers to protect and ensure the safety and/or health of prisoners, the public, and law enforcement officials; to ensure fair and proper treatment of prisoners during custody and transfer of custody; to assist the USMS in pursuing any necessary inquiry/investigation of complaints, alleged misconduct or criminal activity; to process and pay medical claims; and to perform evaluation duties. For example, relevant records or information may be disclosed to secure the safe and efficient transfer of prisoners to other jurisdictions, to court appearances, or to the designated institution for service of sentence; to ensure that appropriate credit for time in custody is given; that appropriate medical treatment is provided; that all rights of the prisoner, whether statutory, humanitarian, or otherwise, are provided and protected; and to elicit information from which to initiate an inquiry/investigation and/or respond to prisoner complaints and reports of alleged misconduct or criminal activity; or, conversely, to enable those entities to respond to, or provide information relating to, such prisoner complaints or reports of misconduct or criminal activity;

(b) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(c) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(d) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(e) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(f) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(g) To the National Archives and Records Administration for purposes of records management inspections

conducted under the authority of 44 U.S.C. 2904 and 2906;

(h) To federal, state, territorial, local, tribal, foreign or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;

(i) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(j) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PROCEDURES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Information is stored in standard file cabinets. Duplicate copies of certain paper and electronic records are stored on magnetic discs.

RETRIEVABILITY:

Information is retrieved by name and/or number of individual in custody, and/or health care provider. Records retrieved by name or number of health care provider will consist of the provider's address, name and number of prisoners treated, claim number, dates of service, nature of service, amount billed, USMS amount allowed, amount saved, and percentage saved.

SAFEGUARDS:

Paper records are stored in locked files. Access to computerized data is restricted through user identification and discrete password functions. In addition, USMS district and headquarters offices are secured behind locked doors around the clock and access is restricted to USMS personnel with official identification.

All USMS contractors must have personnel security clearances commensurate with the highest level of information processed by the system, in this case Limited Official Use. Encryption technology shall be applied to passwords and symmetric or private asymmetric keys, activities of a system administrator or for system maintenance, and information stored on laptop computers. All information technology systems within a component are subject to the certification and accreditation process.

RETENTION AND DISPOSAL:

General prisoner records are kept in active files until a prisoner has been transferred from the custody of USMS. After a prisoner leaves USMS custody, the file is closed, and at the end of the year, closed files are separated from active files. Closed files are maintained for one year after separation, then are transferred to a Federal Records Center, and are destroyed after 10 years, or sooner, if ordered by the Court. This does not apply to records maintained by the Contractor, which are discussed below.

The Contractor will maintain all appropriate paper documents (i.e., invoices, etc.) and automated online files for the duration of the contract performance. Computer storage media containing Limited Official Use information will be overwritten or degaussed prior to release of the storage media outside the USMS. At the end of the contract, the contractor shall turn over all paper documents and automated files of the database offline to the USMS within two weeks of contract expiration. All paper documents and automated files of the database will be maintained in accordance with the General Records Schedule 6, Item 1a (Accountable Officers' Files), as published by NARA, unless a longer retention period is necessary because of pending administrative or judicial proceedings.

The retention and disposal procedures for this system of records are in accordance with the NARA disposition authority for the USMS which is NI 527–99–1, or the General Records Schedule as appropriate.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Witness Security and Prisoner Operations, United States Marshals Service, 11th Floor, CS–4, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Requests for access must be in writing and should be addressed to the System Manager named above, Attention: FOI/PA Officer. The envelope and letter should be clearly marked ''Privacy Act Access Request.'' The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled ''Exemptions Claimed for the System.'' An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, Attention: FOI/PA Officer, stating clearly and concisely the identifying information required above in ''Record access procedures'', what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from contesting record procedures as described in the section entitled ''Exemptions Claimed for the

System.'' An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

RECORD SOURCE CATEGORIES:

Information is received from the individual in custody; the courts, federal, state, territorial, local, tribal and foreign law enforcement agencies and personnel; witnesses; and medical care professionals and/or facilities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(1), (2), (3), (e)(5) and (e)(8) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the **Federal Register**. The rules are codified at 28 CFR 16.101(q) and (r).

JUSTICE/USM–006

SYSTEM NAME:

United States Marshals Service Training Files.

SECURITY CLASSIFICATION:

Limited official use.

SYSTEM LOCATION:

a. Primary system: Human Resources Division, United States Marshals Service, CS–3, Washington, DC 20530–1000.

b. Decentralized segments: Individual training files and the Fitness in Total (FIT) Program training assessment files, identified as items (1) and (3) under ''Categories of Records in the System,'' are located also at the USMS Training Academy, Department of Justice, Building 70, Glynco, Georgia 31524. Each district office of the USMS maintains FIT files only on their respective participants in the FIT Program. The addresses of USMS district offices are on the Internet (*http://www.usdoj.gov/marshals/usmsofc.html*).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Trainees hired as Deputy U.S. Marshals and Deputy U.S. Marshals.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Individual training files contain information on the individual's educational background and employee training history, and an individual career development plan; (2) skills files identify languages and other special skills possessed by the individual USMS employee; and (3) individual FIT Program training assessment files contain records on physical and medical examinations, blood tests, health histories, physical assessments, and administrative records on participation, goal setting and progress while in the program. The Certificate of Medical Examination (SF–78) is maintained in the primary system at USMS headquarters only unless obtained and placed in the district file by the individual FIT participant.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 509, 510, and 569; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111(h).

PURPOSE(S):

Individual training files are used to make employment, promotion, or retention determinations for all Deputy U.S. Marshals; to develop training histories; and to determine training and/or promotion eligibility. In addition, FIT Program training assessment files are used to make hiring/retention determinations for Deputy U.S. Marshal personnel entering on duty as of July 1, 1984 and later; to determine employees' eligibility to participate in the program; to tailor an individual fitness program for each employee; to chart employee progress in the program; to determine the need for and to chart progress toward weight reduction; to develop physical fitness standards for performance appraisal purposes; and to examine statistically the physical fitness level of the USMS workforce against law enforcement populations and the general population of the United States. Skills files are used to identify special skills and language abilities possessed by personnel to aid in staffing special assignments which require such skills.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

RECORDS OR INFORMATION MAY BE DISCLOSED AS A ROUTINE USE:

(a) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(c) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(h) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(i) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(j) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel—related or other official

purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Originals of paper records contained in this system are kept in standard file cabinets. Skills files, summaries of FIT Program training assessment records, and duplicates of paper records are stored on magnetic discs.

RETRIEVABILITY:

Records are retrieved by the employee's name.

SAFEGUARDS:

Records are maintained in metal filing cabinets which are locked during non-duty hours. Entry to headquarters is restricted by 24-hour guard service to employees with official and electronic identification. Entry to the Training Academy and district offices is restricted generally to trainees/employees with official identification. Access to computerized records in this system is restricted to the responsible headquarters employees by assigned code.

RETENTION AND DISPOSAL:

Files are maintained for five (5) years then the magnetic disks are erased and paper records are archived in the Federal Records Center and destroyed when 20 years old, unless the employee leaves the USMS at which time paper records are transferred to another agency, or sent to the OPM records center.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Human Resources Division, USMS, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Freedom of Information Act/Privacy Act Request.'' Clearly indicate name of the requester, nature of the record sought, approximate dates of the records, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager listed above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Freedom of Information Act/Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information contained in this system is collected from the individual, training personnel, the Combined Federal Law Enforcement Training Academy, examining physicians, fitness coordinators, and personnel records.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/USMS–008

SYSTEM NAME:

Witness Security Files Information System.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Witness Security and Prisoner Operations, United States Marshals Service (USMS), CS–4, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Government witnesses or potential witnesses and their families authorized to participate in the Witness Security Program.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains requests to enter the Witness Security Program, authorizations to enter the program, identifying and background information on the witness and/or the witness's family, funding information, and moving information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 509, 510, 524, and 561 et seq.; 5 U.S.C. 301; 44 U.S.C. 3101; 28 CFR 0.111(c); 18 U.S.C. 3521.

PURPOSE(S):

The USMS provides for the security, health and safety of government witnesses and their immediate dependants whose lives are in danger as a result of their testimony against organized crime, drug traffickers, terrorists and other major criminals. The Witness Security Files are used to plan and accomplish the major functions involved in the protection of government witnesses and their families.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records or information may be disclosed as follows:

(a) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(b) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(c) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(d) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(e) To an actual or potential party to litigation or the party's authorized

representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(f) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Records are kept in file folders and in a computerized database.

RETRIEVABILITY:

Filed and retrieved by special ID number.

SAFEGUARDS:

Access is restricted to Witness Security personnel using locks and alarm devices, passwords and/or encrypting data communications. The records are located in a restricted area of USMS Headquarters under 24-hour guard protection with entry controlled by official and electronic identification.

RETENTION AND DISPOSAL:

Witness case files will be closed upon witness termination from the Witness Security Program and retained in the custody of the USMS for 15 years, thereafter they will be transferred to the Federal Records Center and destroyed 75 years after termination. Financial records are destroyed after three years and three months in accordance with General Records Schedules 6, 7 and 8.

SYSTEM MANAGER(S) AND ADDRESS:

Witness Security and Prisoner Operations, U.S. Marshals Service, CS–4, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as the ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Privacy Act Request.'' Clearly indicate name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager listed above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information is provided by the witnesses and their families, the court, federal, state, territorial, local, tribal and foreign law enforcement agencies, and medical personnel.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(2) and (3), (e)(4)(G) and (H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the **Federal Register**. See 28 CFR 16.101.

JUSTICE/USM–009

SYSTEM NAME:

Inappropriate Communications/ Threat Information System.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Primary System: Investigative Services Division, U.S. Marshals Service (USMS), CS–4, Washington, DC 20530–1000.

Decentralized Segments: Each district office of the USMS maintains their own files. The addresses of USMS district offices are available on the Internet at *http://www.usdoj.gov/marshals/usmsofc.html.*

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have inappropriately communicated with, directly threatened, or pose a threat to USMS protectees, including federal judges, prosecutors, and other court officials. U.S. Marshals, deputies and other law enforcement officers, courtroom security, and federal property and buildings; associates of the threat or inappropriate communication initiator; and individuals reported by state or local agencies to the USMS who have threatened to harm state or local judicial officials.

CATEGORIES OF RECORDS IN THE SYSTEM:

Manual and automated records which consist of information related to the inappropriate communication or threat, including type of communication, the means by which it was issued, and information contained in the communication such as dates, locations, and events; analysis of the communication or threat and other internal USMS correspondence relating to the communication; biographical data including physical description,

photograph, and criminal history information—in particular, known history of violence and skills related to the nature of the threat; investigative information including associations with other individuals and dangerous gangs, extremist groups, or other organizations; information on associates including physical descriptions, photographs, numerical identifiers, addresses, driver's license information; and investigative information furnished by other federal, state, territorial, tribal, and local law enforcement or other government agencies and non-government sources.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 509, 510, and 561 *et seq.*; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 111(c) through (f).

PURPOSE(S):

The USMS is required to protect government witnesses, U.S. Attorneys and their assistants, federal jurists and other court officers; to provide for courtroom security; and to assist in protecting federal property and buildings. The USMS also conducts Federal law enforcement activities itself, *e.g.*, warrant apprehension investigations, which subject its officers to security danger. These operations require acquiring information to allow an accurate assessment of the existence and extent of the dangers posed, including specific threats, to aid in responding to specific security assignments and needs, as well as developing protective measures and plans in advance. With the information collected, officials determine and carry out operating plans, funding, personnel, and any special resources needed to counteract threat situations.

Individuals reported by State and local agencies to the USMS who have threatened to harm state or local judicial officials often appear before the federal bar as a result of appeals, civil rights suits, continuing criminal behavior, etc. Such individuals may continue their inappropriate communications or threats at the federal level. In that event, information concerning these individuals provided by the state and local agencies assists the USMS in assessing the dangers they pose to federal officials and in developing protective measures and responding to specific security requirements. This information also assists in researching inappropriate communications directed toward judicial officials of all jurisdictions to gain a full and comprehensive picture of the diverse circumstances involved, to analyze trends based upon a statistically reliable study, and to more fully address the problem.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Records or information may be disclosed:

(a) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) To other law enforcement agencies to develop protective measures where a specific threat is posed to their members; and to an individual or organization where the recipient is or could become the target of a specific threat;

(c) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(h) To federal, state, territorial, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;

(i) A record may be disclosed to designated officers and employees of state, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(j) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:

Paper records are kept in file folders. Duplicate copies of paper records are stored on magnetic discs.

RETRIEVABILITY:

Records are retrieved by name and identifying number or a combination of the name and number.

SAFEGUARDS:

Except as otherwise noted in paragraphs (a) and (b) under ''Routine uses,'' access to computerized records is restricted to personnel in the Investigative Services Division and in each district office by user identification and password. Paper records are maintained in filing cabinets within supervised areas. District and headquarters offices are locked during working and non-duty hours and entry is restricted to employees with official identification.

RETENTION AND DISPOSAL:

Headquarters files are destroyed one year after the initiator of the threat or inappropriate communication is no longer active or the case has been closed. District files are destroyed five years after the initiator of the threat or inappropriate communication is no longer active or the case has been closed.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Investigative Services Division, U.S. Marshals Service, CS–4, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as ''Record access procedure.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Freedom of Information/Privacy Act Request.'' Clearly indicate name of the requester, nature of the record sought, approximate date of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager identified above. State clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Freedom of Information/Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information is obtained from public and confidential sources, the threat or inappropriate communication initiator, and from federal, state and local law enforcement agencies.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the **Federal Register.** See 28 CFR 16.101.

JUSTICE/USM–010

SYSTEM NAME:

Judicial Facility Security Index System.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Judicial Security Division, United States Marshals Service (USMS), CS–3, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals employed, or offered employment as contract court security officers (CSO's) by companies contracting with the USMS to provide judicial area security in federal courthouses and USMS facilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

An alphabetical index contains the name, date of birth and social security number of the CSO, name of the contracting security firm (employer), completion dates and cost data for limited background investigation and orientation, district of employment, dates contract performance started and ended, posts and hours of duty and the status of employment, i.e., active or inactive. For inactive CSO's, the index contains the reason for inaction, e.g., CSO resigned; applicant rejected based on the preliminary records check; CSO removed based on Office of Personnel Management (OPM) background investigation; etc. In addition to providing abbreviated data, the index assists in locating records on the CSO related to the initial screening process for eligibility, e.g., application and preliminary checks for arrest records, which are filed under the contract number and name of the contracting security firm (employer). The index also assists in locating files containing OPM reports on the limited background investigation and internal suitability memoranda which are segregated by categories ''active'' and ''inactive.''

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 509, 510 and 561 *et seq.;* 5 U.S.C. 301; 44 U.S.C. 3101 and 28 CFR 0.111.

PURPOSE(S):

The USMS administers and implements courtroom security requirements for the federal judiciary and provides assistance in the protection of federal property and buildings. The Judicial Facility Security Program provides uniformed security officers and security systems and equipment for judicial area security in federal courthouses throughout the country. It is funded by the Judiciary through the Administrative Office of the U.S. Courts (AOUSC) and is managed by the USMS. This system of records is used to make security/suitability determinations in the hiring of CSO's, to monitor orientation and training, to track costs related to background investigations and attendance at Government-sponsored orientation, and to monitor contractor performance. It enables program officers to compile data for reports to AOUSC on actual and projected expenses, to list CSO's, their posts and hours of duty, and to determine turnover and reemployment ratios among CSO's.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records may be disclosed as follows:

(a) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized

representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(g) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(h) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(i) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(j) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

An index record is stored on magnetic disks and original paper records are kept in file folders.

RETRIEVABILITY:

Records are retrieved by name of the contract CSO or contractor.

SAFEGUARDS:

Records are stored in locked metal filing cabinets during off-duty hours. Access to computerized records is controlled by restricted code to personnel on a need-to-know basis. Entry to USMS Headquarters is restricted by 24-hour guard service to employees with official and electronic identification.

RETENTION AND DISPOSAL:

Records are maintained indefinitely until a detailed records retention plan and disposal schedule is developed by the National Archives and Records Administration and the USMS.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Judicial Facility Security Program, Judicial Security Division, U.S. Marshals Service, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURES:

Same as the ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark the letter and envelope ''Freedom of Information/Privacy Act Request.'' Clearly indicate name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager listed above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Freedom of Information/Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information contained in this system is collected from the individual, USMS orientation records, other law enforcement agencies, OPM and from the contractor (employer).

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (d) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the **Federal Register**. See 28 CFR 16.101.

JUSTICE/USM–011

SYSTEM NAME:

Judicial Protection Information System.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Primary System: Judicial Security Division, United States Marshals Service (USMS), CS–3, Washington, DC 20530–1000.

Decentralized Segments: Each USMS district office maintains their own files. The addresses of the USMS district offices are available on the Internet at *http://www.usdoj.gov/marshals/usmsofc.html*.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have been directly threatened or are subject to violent threat by virtue of their responsibilities within the judicial system, e.g., U.S. Attorneys and their assistants, federal jurists and other court officials.

CATEGORIES OF RECORDS IN THE SYSTEM:

Manual and automated indices contain abbreviated data, e.g., case number, name of protected subject, name of control district and district number, an indication of the type and source of threat, and the means by which the threat was made. In addition to the abbreviated data named above, the complete file may contain descriptive physical data of the protectee, and other information to identify security risks and plan protective measures in advance of or during periods of active protection, e.g., individual practices and routines,

including associational memberships. Information regarding the expenditure of funds and allocation of resources assigned to the protectee may also be included in the file to enable officials to develop operating plans to counteract threat situations.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

28 U.S.C. 509, 510 and 561 *et seq.*, 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111 (c) through (f).

PURPOSE:

The USMS is required to protect U.S. Attorneys and their assistants, federal jurists and other court officers; to provide for courtroom security, and to assist in protecting federal property and buildings. This operation requires obtaining information to allow an accurate assessment of the individual security needs of such threatened persons to aid in developing protective measures and advance planning of specific security assignments. With the information collected, USMS officials determine and carry out operating plans, funding, personnel assignments and any special resources needed to counteract specific threat situations.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records or information may be disclosed:

(a) To other federal, state and local law enforcement agencies to the extent that disclosure is necessary to develop and/or implement protective measures;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

An index record is stored on index cards and magnetic tape. Original paper records are kept in file folders.

RETRIEVABILITY:

Records are indexed and retrieved by name of protectee.

SAFEGUARDS:

Access to computerized records is restricted to Court Security Program personnel by assigned user code and password. In addition, records are stored in locked metal cabinets during off-duty hours. The records are located in a restricted area, and USMS Headquarters is under 24-hour guard protection with entry controlled by official and electronic identification.

RETENTION AND DISPOSAL:

Records are maintained indefinitely until a detailed records retention plan and disposal schedule is developed by the National Archives and Records Administration and the USMS.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Court Security Program, Judicial Security Division, U.S. Marshals Service, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as the ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Freedom of Information/Privacy Act Request.'' Clearly indicate the name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager identified above. State clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Freedom of Information/Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information is obtained from individual protectees; federal, state, and local law enforcement agencies; public

and confidential sources; and threat initiator.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/USM–013

SYSTEM NAME:

U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files

SECURITY CLASSIFICATION:

Limited Official Use

SYSTEM LOCATION:

Office of General Counsel, U.S. Marshals Service (USMS), CS–3, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have filed tort and employee claims against the USMS; individuals who have initiated administrative proceedings against the USMS; individuals who have filed civil suits naming the USMS and/or personnel as defendants, including those suits arising from authorized criminal law enforcement activities; individuals named as defendants in federal court actions initiated by the USMS; and USMS attorneys assigned to defend such claims and litigation.

CATEGORIES OF RECORDS IN THE SYSTEM:

In addition to the names of individuals covered by the system and the title of cases, a computerized case tracking system contains certain summary data, e.g.; a summary of correspondence and pleadings received in a case, names of parties involved; names of attorneys handling the case or matter, court in which action is brought, and civil action number, thereby facilitating location of the complete file. Cases or matters include adverse actions, grievances, unfair labor practice charges, tort claims, Equal Employment Opportunity and other employee claims, and suits against USMS employees in their official capacities, etc. Files contain correspondence/claim forms submitted by claimants and internal reports and related documents concerning the merits of the claim, attorney or staff recommendations and findings related to the claim; records on actions taken by USMS giving rise to appeals, attorney notes, recommendations and strategy for defending appeals; copies of civil actions filed and criminal investigative records related to the action, e.g., criminal investigative reports relating the underlying criminal matter which relates to or constitutes the basis of the claim or suit (including those from non-Federal law enforcement participants in USMS criminal or civil law enforcement activities), witness statements, reports of interviews, exhibits, attorney notes, pleadings, and recommendations and strategy for defending civil actions.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and 44 U.S.C. 3101.

PURPOSE(S):

Among other responsibilities, the Office of General Counsel, U.S. Marshals Service, provides legal representation to USMS management in all administrative matters including, but not limited to, adverse actions, grievances, unfair labor practices, EEO, tort and employee claim proceedings; represents the Service and its employees in district court actions brought against them for acts taken in the course of official duties; and represents the Service in other actions in which its interests are involved. Effective representation in such matters requires that records be retrievable by individual identifiers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records maintained in this system of records may be disseminated as follows:

(a) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) To any federal, state or local agency, organization or individual to the extent necessary to elicit information or witness cooperation if there is reason to believe the recipient possesses information related to the case or matter;

(c) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(d) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(e) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(f) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(g) To the news media and the public including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(h) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(i) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(j) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipients agency's decision;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee

regarding a matter within that persons former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

STORAGE:

Administrative claim, appeal, and litigation files are stored in standard file cabinets. The computerized case tracking system and duplicate copies of some paper records are stored on magnetic discs.

RETRIEVABILITY:

Records are retrieved by name of claimant, litigant or USMS attorney, or by caption of civil action or administrative proceeding.

SAFEGUARDS:

Access to computerized records is restricted to Office of General Counsel personnel by user identification and passwords. In addition, files are stored in metal filing cabinets within the Office of General Counsel, USMS Headquarters during off-duty hours. Access to USMS Headquarters is restricted to employees with official identification.

RETENTION AND DISPOSAL:

Records in the case tracking system are retained indefinitely. Claim files are destroyed after 7 years. Litigation files are destroyed after 10 years. Cases designated by the General Counsel as significant or precedential are retained indefinitely.

SYSTEM MANAGER(S) AND ADDRESS:

General Counsel, Office of General Counsel, U.S. Marshals Service, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Freedom of Information/Privacy Act Request.'' Clearly indicate name of the requester, nature of the record sought, approximate dates of the records, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above. Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager listed above. State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Freedom of Information/ Privacy Act Request.''

RECORD SOURCE CATEGORIES:

The sources of information contained in this system are the individual claimant/litigant, USMS officials, law enforcement agencies, statements of witnesses and parties, transcripts of depositions and court proceedings, administrative hearings and arbitrations, and work product of staff attorneys and legal assistants working on a particular case or matter.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted certain categories of records in this system from subsections (c)(3) and (4); (d); (e)(2) and (3); (e)(4)(G) and (H); (e)(8); (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) or (k)(5). The system is exempted pursuant to subsection (j)(2) only to the extent that information in a record pertaining to a particular individual relates to a criminal investigation which relates to or constitutes the basis of a particular suit or claim. The system is exempted pursuant to subsection (k)(5) only to the extent necessary to protect a confidential source. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the **Federal Register**. See 28 CFR 16.101.

JUSTICE/USM–016

SYSTEM NAME:

U.S. Marshal Service (USMS) Key Control Record System.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Primary system: Judicial Security Division, United States Marshals Service, CS–3, Washington, DC 20530.

Decentralized segments: USMS headquarters division offices that issue keys to their respective employees.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former employees of the USMS who have been issued building or office keys for USMS Headquarters or District Office locations.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records contained in this system consist of an automated or manual index which may include the name of the employee to whom a building or office key is issued; the social security number (only when two or more employees have identical names, including middle initial); unique key identification code number; key type (e.g., grand master, master, submaster, change); storage container hook number; description (e.g., number identification) of door(s), room(s), and/or area(s) the key opens or accesses; transactions type and/or status (e.g., key issued, transferred, retrieved, lost, broken) and transaction date; and, any other appropriate comment, e.g., comments regarding key, door, room, area, etc.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and 44 U.S.C. 3101.

PURPOSE(S):

The USMS Key Control Record System serves as a record of keys issued and facilitates continuing security at USMS Headquarters locations. Records are maintained to assist in restricting office and work area access to authorized USMS personnel by controlling, monitoring and tracking keys issued. In addition, the records assist in identifying any repairs, changes, or additional security measures that may be necessary as a result of lost or broken keys.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

RECORDS OR INFORMATION MAY BE DISCLOSED:

(a) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or

prosecuting such violation or enforcing or charged with implementing such law;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Automated index records are stored on magnetic disks. Paper copies of automated records are kept in file folders and original paper records of the manual index are stored in card files.

RETRIEVABILITY:

Records are retrieved by name of the individuals covered by the system.

SAFEGUARDS:

Access to these records is restricted to personnel of the USMS, Office of Security. Computerized records may be accessed only by assigned code and password. Paper records are located in a restricted area and are maintained in metal filing cabinets or safes which are locked during non-duty hours.

RETENTION AND DISPOSAL:

Records are retained for three years after turn-in of the key at which time they are destroyed (General Records Schedule 18).

SYSTEM MANAGER(S) AND ADDRESS:

Judicial Security Division, United States Marshals Service, CS–3, Washington, DC 20530.

NOTIFICATION PROCEDURE:

Same as the ''Records access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Freedom of Information/Privacy Act Request.'' Clearly indicate the name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager listed above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Freedom of Information/Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information contained in this system is collected from the individual and the system manager.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/USM–017

SYSTEM NAME:

Judicial Security Staff Inventory.

SECURITY CLASSIFICATION:

Limited Official Use.

SYSTEM LOCATION:

Judicial Security Division (JSD), U.S. Marshals Service (USMS), CS–3, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

USMS employees, contract employees, and other individuals assigned to JSD.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records contained in this computerized system consist of (1) an individual's name, date of birth, social security number, and type of passport with expiration date; (2) inventory of accountable property assigned to individual, including: weapon, protective body armor with expiration date of warranty, vehicle, credit cards, cell phone, pager, and office equipment.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 28 U.S.C. 509 and 510; 44 U.S.C. 3101 and 28 CFR 0.111.

PURPOSE(S):

This system will be used to assist JSD management in the effective control of accountable property and to ensure that JSD personnel maintain the equipment necessary and in proper working order to perform their functions, especially law enforcement functions, and to respond quickly to urgent operational law enforcement activities as they develop.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

RECORDS OR INFORMATION MAY BE DISCLOSED:

(a) Where a record, either alone or in conjunction with other information,

indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To the news media and the public, including disclosure pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Departments efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Records are kept in a computerized database.

RETRIEVABILITY:

Information is retrieved by name and social security number.

SAFEGUARDS:

Access is limited to designated staff of JSD by assigned user code and password. JSD is located in a restricted area of USMS Headquarters which is under 24–hour guard protection with entry controlled by official and electronic identification.

RETENTION AND DISPOSAL:

Files are maintained until the employee leaves JSD at which time all records on the individual will be erased from the database.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Judicial Security Division, U.S. Marshals Service, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as the ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Privacy Act Request.'' Clearly indicate the name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager identified above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope ''Privacy Act Request.''

RECORD SOURCE CATEGORIES:

Information is obtained from subject JSD employees, JSD office and the accountable property records.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/USM–018

SYSTEM NAME:

United States Marshals Service Alternative Dispute Resolution (ADR) Files and Database Tracking System.

SECURITY CLASSIFICATION:

Limited official use.

SYSTEM LOCATION:

Human Resources Division, United States Marshals Service (USMS), CS–3, Washington, DC 20530–1000.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Employees of the USMS designated as complainants, who select ADR mediation as the mechanism to resolve disagreements, and designated respondents to such complaints.

CATEGORIES OF RECORDS IN THE SYSTEM:

ADR files contain a statement of issue(s) which include type of dispute, parties involved, and date ADR requested or notified by complainant; mediator appointed; correspondence or letters which may include ground rules, acknowledgment of time requirements and issues related thereto; pre-conference agreements; minutes of ADR activity; written agreement, and dispute resolution and date resolved.

The ADR data tracking system contains names of complainant and respondent; type of dispute, e.g., job assignment, leave, promotion; source of complaint, e.g., Equal Employment Opportunity (EEO) or grievance; process utilized, e.g., mediation, conciliation, fact finding; district/office; ADR contact individual; date ADR request received;

date resolved; and calculation of time spent in resolving matters and, if applicable, name of mediator.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and 44 U.S.C. 3101.

PURPOSE(S):

The ADR process is a parallel system to the grievance process and Equal Employment Opportunity (EEO) complaint process which offers the possibility of a simpler, quicker, less expensive, and less adversarial resolution of disputes. The ADR files are used to facilitate the effective operation of the ADR process in resolving discrimination complaints and workplace grievances by USMS employees and applicants for employment. The ADR database is used to track case activity, primarily for completion of reports.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

RECORDS OR INFORMATION MAY BE DISCLOSED:

(a) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings;

(g) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit;

(h) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(i) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(j) To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

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

STORAGE:

Records are stored in standard file cabinets. Computerized records are stored in a database server in a secured file room.

RETRIEVABILITY:

Records are retrieved by name of employee.

SAFEGUARDS:

Access is restricted to authorized personnel with the need to know in the Human Resources Division, Equal Employment Opportunity Division, and the Office of General Counsel. Computerized records may be accessed only by assigned code and password. In addition, records are stored in metal file cabinets within the Human Resources Division and access to USMS headquarters is controlled by 24-hour guard services.

RETENTION AND DISPOSAL:

Records are maintained for 7 years and then data in the system, as well as hard copies, are purged.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Human Resources Division, USMS, CS–3, Washington, DC 20530–1000.

NOTIFICATION PROCEDURE:

Same as ''Record access procedures.''

RECORD ACCESS PROCEDURES:

Make all requests for access in writing and clearly mark letter and envelope ''Privacy Act Request.'' Clearly indicate name of the requester, nature of the record sought, approximate dates of the records, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information to the system manager in accordance with the procedures outlined above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Employee complainants, who select the ADR process to resolve their disputes; respondents; and the ADR mediator.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E7–11543 Filed 6–15–07; 8:45 am]

BILLING CODE 4410–04–P

DEPARTMENT OF LABOR

Office of the Secretary

Job Corps: Preliminary Finding of No Significant Impact (FONSI) for the Proposed Job Corps Center To Be Located North of Roosevelt Highway Between Washington Road and Interstate 285 in College Park, GA

AGENCY: Office of the Secretary (OSEC), Department of Labor.

ACTION: Preliminary Finding of No Significant Impact (FONSI) for the Proposed Job Corps Center to be located north of Roosevelt Highway between Washington Road and Interstate 285 in College Park, Georgia.

SUMMARY: Pursuant to the Council on Environmental Quality Regulations (40 CFR part 1500–08) implementing procedural provisions of the National Environmental Policy Act (NEPA), the Department of Labor, Office of the Secretary (OSEC), in accordance with 29 CFR 11.11(d), gives notice that an Environmental Assessment (EA) has been prepared for a proposed new Job Corps Center to be located in College Park, Georgia, and that the proposed plan for a new Job Corps Center will have no significant environmental impact. This Preliminary Finding of No Significant Impact (FONSI) will be made available for public review and comment for a period of 30 days.

DATES: Comments must be submitted by July 18, 2007.

ADDRESSES: Any comment(s) are to be submitted to Michael F. O'Malley, Office of the Secretary (OSEC), Department of Labor, 200 Constitution Avenue, NW., Room N–4460, Washington, DC 20210, (202) 693–3108 (this is not a toll-free number).

FOR FURTHER INFORMATION CONTACT: Copies of the EA are available to interested parties by contacting Michael F. O'Malley, Architect, Unit Chief of Facilities, U.S. Department of Labor, Office of the Secretary (OSEC), 200 Constitution Avenue, NW., Room N–4460, Washington, DC 20210, (202) 693–3108 (this is not a toll-free number).

SUPPLEMENTARY INFORMATION: This Environmental Assessment (EA) summary addresses the proposed construction of a new Job Corps Center near College Park, Georgia. The site for the proposed Job Corps Center is comprised of four parcels of land owned by VFH Captive Insurance Company which total approximately 25.4 acres. The property is currently undeveloped and wooded with the exception of three abandoned residential properties and an abandoned automotive repair garage.

The new center will require construction of ten (10) buildings including eight (8) single-story buildings and two (2) two-story buildings. The proposed Job Corps center will provide housing, training, and support services for approximately 515 students. The current facility utilization plan includes include a vocational-educational building, cafeteria/culinary arts building, child development center, recreation building, medical/dental building, maintenance/warehouse building, administration offices, and new dormitories.

The construction of the Job Corps Center on this proposed site would be a positive asset to the area in terms of environmental and socioeconomic improvements, and long-term productivity. The proposed Job Corps Center will be a new source of employment opportunity for people in the Atlanta Metropolitan area. The Job Corps program provides basic education, vocational skills training, work experience, counseling, health care and related support services. The program is designed to graduate students who are ready to participate in the local economy.

The proposed project will not have any significant adverse impact on any natural systems or resources. No state or federal threatened or endangered species (proposed or listed) have been identified on the subject property.

The Job Corps Center construction will not affect any existing historic structures, as there are no historic or archeologically sensitive areas on the proposed property parcel.

Air quality and noise levels should not be affected by the proposed development project. Due to the nature of the proposed project, it would not be a significant source of air pollutants or additional noise, except possibly during construction of the facility. All construction activities will be conducted in accordance with applicable noise and air pollution regulations, and all pollution sources will be permitted in accordance with applicable pollution control regulations.

The proposed Job Corps Center is not expected to significantly increase the vehicle traffic in the vicinity, since many of the Job Corps Center residents will either live at the Job Corps Center or use public transportation. While some Job Corps Center students and staff may use personal vehicles, their number would not result in a significant increase in vehicular traffic in the area. Access is planned from Roosevelt Highway. Road improvements and/or installation of signals to facilitate site ingress/egress do not appear necessary. Public transportation will be provided by Metropolitan Atlanta Rapid Transit Authority which provides bus and shuttle routes throughout Metropolitan Atlanta. Bus Route 88 travels along Washington Road which bounds the west side of the proposed Job Corp Center site. There are a number of connecting bus routes within walking distance of the site.

The proposed project will not have any significant adverse impact on the surrounding water, sewer, and storm water management infrastructure. The new buildings to be constructed for the proposed Job Corps Center will be tied in to the existing City of Atlanta Watershed Management system. The new buildings to be constructed for the proposed Job Corps Center will also be tied in to the existing Fulton County wastewater treatment system.

Georgia Power would provide the electricity for the site. This is not expected to create any significant impact to the regional utility infrastructure.

No significant adverse affects to local medical, emergency, fire, and police services are anticipated. The primary medical provider located closest to the proposed Job Corps parcel is South Fulton Medical Center, approximately 6 miles from the proposed Job Corps Center. Nevertheless, the Job Corps center will have a small medical and dental facility as part of the campus for use by the residents, as necessary for providing a ward for sick students with the flu or small non-emergency incapacities. Security services at the Job Corps will be provided by the center's security staff. Law enforcement services are provided by the Fulton County Police Department, located