



Billing Code 4410-NW

**DEPARTMENT OF JUSTICE**

**CPCLO Order No. 005-2017**

**Privacy Act of 1974; System of Records**

**AGENCY:** United States Department of Justice.

**ACTION:** Notice of Modified Systems of Records.

**SUMMARY:** Pursuant to the Privacy Act of 1974, and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the United States Department of Justice (Department or DOJ) proposes to modify the DOJ System of Records Notices for the DOJ systems of records listed below.

**DATES:** In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is subject to a 30-day notice and comment period. Please submit any comments by **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** The public, OMB, and Congress are invited to submit any comments to the U.S. Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW, Suite 1000, Washington, DC 20530-0001, by facsimile at 202-307-0693, or email at [privacy.compliance@usdoj.gov](mailto:privacy.compliance@usdoj.gov). To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

**FOR FURTHER INFORMATION CONTACT:** Andrew A. Proia, Attorney Advisor, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW, Suite 1000, Washington, DC 20530-0001, by facsimile at 202-307-0693, or

email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

**SUPPLEMENTARY INFORMATION:**

On May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, to the heads of all executive departments and agencies. In its memorandum, OMB required agencies to publish a routine use for their systems of records specifically addressing the disclosure of records in connection with the response to, and remedial efforts in the event of, a breach of personally identifiable information. DOJ published a notice in the Federal Register, 72 FR 3410 (January 25, 2007), modifying all DOJ System of Records Notices by adding a routine use to address the limited disclosure of records related to a suspected or confirmed breach within the Department, consistent with OMB requirements. Since that time, all new DOJ System of Records Notices published by the Department, as well as significantly modified System of Records Notices that were republished in full, included a breach response routine use consistent with the requirements in OMB Memorandum M-07-16.

On January 3, 2017, OMB issued Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, to the heads of all executive departments and agencies. OMB Memorandum M-17-12 rescinds and replaces OMB Memorandum M-07-16 and updates agency routine use requirements for responding to a breach. Specifically, OMB Memorandum M-17-12 requires all Senior Agency Officials for Privacy to ensure that their agency's System of Records Notices include a routine use for the disclosure of information necessary to respond to a breach of

the agency's personally identifiable information. Additionally, OMB Memorandum M-17-12 requires agencies to add a routine use to ensure that agencies are able to disclose records in their systems of records that may reasonably be needed by another agency in responding to a breach.

To satisfy the routine use requirements in OMB Memorandum M-17-12, DOJ is issuing two notices in the Federal Register to modify all of the Department's System of Records Notices. The records maintained in many DOJ systems of records are still subject to the Department's blanket breach response routine use published at 72 FR 3410 (January 25, 2007). As a result, elsewhere in the Federal Register, the Department is rescinding 72 FR 3410 (January 25, 2007) and modifying all of the DOJ System of Records Notices for the DOJ systems of records still subject to the Department's blanket breach response routine use published at 72 FR 3410 (January 25, 2007). These System of Records Notices are not affected by this notice publication. The DOJ System of Records Notices for these DOJ systems of records are being modified separately to ensure continuity with their previous notice publications.

Pursuant to OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017), this notice: (1) revises the breach routine use for the DOJ systems of records, listed below; and (2) adds a new routine use to the DOJ systems of records, listed below, to ensure that the Department can assist another agency in responding to a confirmed or suspected breach, as appropriate. This notice also includes administrative clarifications to the security classification of two DOJ System of Records Notices for DOJ systems of records, one maintained by the International Criminal Police Organization (INTERPOL) Washington, United States

National Central Bureau (USNCB), and the other by the Justice Management Division (JMD).

Other DOJ systems of records have been created or significantly modified since 72 FR 3410 (January 25, 2007) added the previous, OMB-required breach response routine use. The DOJ System of Records Notices for these DOJ systems of records incorporated the OMB Memorandum M-07-16 breach response routine use in their “ROUTINE USES” section, rather than relying on the routine use published at 72 FR 3410 (January 25, 2007). Specifically, these DOJ System of Records Notices are:

JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records;

JUSTICE/DOJ-013, Justice Federal Docket Management System [Justice FDMS];

JUSTICE/DOJ-014, Department of Justice Employee Directory Systems;

JUSTICE/DOJ-015, Department of Justice Employee Assistance Program (EAP) Records;

JUSTICE/DOJ-016, Debt Collection Enforcement System;

JUSTICE/DOJ-017, Department of Justice, Giglio Information Files;

JUSTICE/COPS-002, COPS Online Ordering System;

JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records;

JUSTICE/CRM-029, United States Victims of State Sponsored Terrorism Fund (USVSSTF) File System;

JUSTICE/DEA-008, Investigative Reporting and Filing System;

JUSTICE/FBI-009, The Next Generation Identification (NGI) System;

JUSTICE/FBI-019, Terrorist Screening Records Center (TSRS);

JUSTICE/FBI-020, Law Enforcement National Data Exchange System (NDEX);

JUSTICE/FBI-022, FBI Data Warehouse System;

JUSTICE/INTERPOL-001, INTERPOL-United States National Central Bureau (USNCB) Records System;

JUSTICE/JMD-003, Department of Justice Payroll System;

JUSTICE/NSD-001, Foreign Intelligence and Counterintelligence Records System;

JUSTICE/NSD-002, Registration and Informational Material Files Under the Foreign Agents Registration Act of 1938;

JUSTICE/NSD-003, Registration Files of Individuals Who Have Knowledge of, or Have Received Instruction or Assignment in, Espionage, Counterespionage, or Sabotage Service or Tactics of a Foreign Government or of a Foreign Political Party;

JUSTICE/OCDETF-001, Organized Crime Drug Enforcement Task Forces Management Information System;

JUSTICE/OCDETF-002, Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System;

JUSTICE/OIG-001, Office of the Inspector General Investigative Records;

JUSTICE/OPA-001, Executive Clemency Case Files/Executive Clemency Tracking System;

JUSTICE/OPR-001, Office of Professional Responsibility Record Index;

JUSTICE/OVW-001, Peer Reviewer Database;

JUSTICE/USM-001, U.S. Marshals Service Badge & Credentials File;

JUSTICE/USM-002, Internal Affairs System;

JUSTICE/USM-004, Special Deputation Files;

JUSTICE/USM-005, U.S. Marshals Service Prisoner Processing and Population Management-Prisoner Tracking System (PPM-PTS);

JUSTICE/USM-006, United States Marshals Service Training Files;

JUSTICE/USM-007, Warrant Information Network (WIN);

JUSTICE/USM-008, Witness Security Files Information System;

JUSTICE/USM-009, Inappropriate Communications- Threat Information System;

JUSTICE/USM-010, Judicial Facility Security Index System;

JUSTICE/USM-011, Judicial Protection Information System;

JUSTICE/USM-013, U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files;

JUSTICE/USM-016, U.S. Marshals Service (USMS) Key Control Record System;

JUSTICE/USM-017, Judicial Security Staff Inventory; and

JUSTICE/USM-018, United States Marshals Service Alternative Dispute Resolution (ADR) Files and Database Tracking System.

This notice modifies the “ROUTINE USES” section of the DOJ System of Records Notices, listed above. Additionally, this notice includes an administrative change to an INTERPOL System of Records Notice titled, JUSTICE/INTERPOL-001, “INTERPOL-United States National Central Bureau (USNCB) Records System,” last published in full at 75 FR 27821 (May 18, 2010), and a JMD System of Records Notice titled, JUSTICE/JMD-003, “Department of Justice Payroll System,” last published in full

at 69 FR 107 (January 2, 2004). This notice adds the “SECURITY CLASSIFICATION” section to both DOJ System of Records Notices. This section was not previously published in these System of Records Notices.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and to Congress on this notice of modified systems of records.

5-19-2017

Date

Peter A. Winn

Acting Chief Privacy and Civil Liberties Officer  
United States Department of Justice

**JUSTICE/DOJ-004**

**SYSTEM NAME AND NUMBER:**

JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records.

**SECURITY CLASSIFICATION:**

Unclassified and classified information.

**SYSTEM LOCATION:**

United States Department of Justice, 950 Pennsylvania Ave. NW., Washington, DC 20530-0001, and other Department of Justice offices throughout the country.

**SYSTEM MANAGER(S) AND ADDRESS:**

Chief of Staff, Office of Information Policy, United States Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (p) as follows:]

(p) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (r) as follows:]

(r) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

77 FR 26580 (May 4, 2012): Last published in full.

**JUSTICE/DOJ-013**

**SYSTEM NAME AND NUMBER:**

JUSTICE/DOJ-013, Justice Federal Docket Management System [Justice FDMS].

**SECURITY CLASSIFICATION:**

None.

**SYSTEM LOCATION:**

U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530 and other Department of Justice offices.

**SYSTEM MANAGER(S) AND ADDRESS:**

*Technical Issues:* Justice Department, Deputy Chief Information Officer for EGovernment, Office of the Chief Information Officer, United States Department of Justice, 950 Pennsylvania Avenue, NW., RFK Main Building, Washington, DC 20530.

*Policy Issues:* Justice Department FDMS Policies System Administrator, Office of Legal Policy, United States Department of Justice, 950 Pennsylvania Avenue, NW., RFK Main Building, Washington, DC 20530.

*Component Managers* can be contacted through the Department's System Managers.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use N. and add routine use M. as follows:]

N. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

M. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient

agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 12196 (March 15, 2007): Last published in full.

**JUSTICE/DOJ-014**

**SYSTEM NAME AND NUMBER:**

JUSTICE/DOJ-014, Department of Justice Employee Directory Systems.

**SECURITY CLASSIFICATION:**

Sensitive But Unclassified Information and/or Controlled Unclassified Information

**SYSTEM LOCATION:**

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530–0001, and other Department of Justice offices throughout the United States and abroad.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Office of Privacy and Civil Liberties, Department of Justice, National Place Building, 1331 Pennsylvania Avenue, NW., Suite 940, Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (f) as follows:]

(f) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (l) as follows:]

(l) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

74 FR 57194 (November 4, 2009): Last published in full.

## **JUSTICE/DOJ-015**

### **SYSTEM NAME AND NUMBER:**

JUSTICE/DOJ-015, Department of Justice Employee Assistance Program (EAP) Records.

### **SECURITY CLASSIFICATION:**

Unclassified.

### **SYSTEM LOCATION:**

Employee Assistance Program (EAP) records are located at the U.S. Department of Justice, 1331 Pennsylvania Avenue NW., Washington, DC 20530, and other Department of Justice (DOJ) offices throughout the country. For those components that operate component-specific EAPs, records are located at the component's primary location and/or its field division sites. The main address for each DOJ component is posted on the DOJ Web site, *www.justice.gov*. EAP records for components that utilize contractors in providing EAP services may also be maintained by such contractors, on behalf of the Department, at the contractor's location. To determine the location of particular EAP records, contact the appropriate EAP Privacy Act system manager, whose contact information is listed below in the System Managers and Addresses section.

### **SYSTEM MANAGER(S) AND ADDRESS:**

EAP records are located at various DOJ-operated and contractor-operated facilities. Six components of the DOJ operate component-specific EAPs. The primary Privacy Act system manager and address for component-specific EAPs are as follows:

ATF: EAP Administrator, Human Resources Division, Bureau of Alcohol, Tobacco, Firearms, and Explosives, 99 New York Ave. NE., Washington, DC 20226.

DEA: EAP Administrator, Drug Enforcement Administration, 8701 Morrisette Drive Springfield, VA 22152.

EOUSA: EAP Administrator, Executive Office for United States Attorneys, 600 E St. NW., Room 2800, Washington, DC 20530.

FBI: EAP Administrator, Federal Bureau of Investigation, 935 Pennsylvania Ave. NW., Room 10190, Washington, DC, 20535-0001.

BOP: EAP Administrator, Federal Bureau of Prisons, 320 First St. NW., Room HOLC-871, Washington, DC 20534.

USMS: EAP Administrator, United States Marshals Service, Room 750, CS-3, Washington, DC 20530.

For all other DOJ components, the primary Privacy Act system manager and address is EAP Administrator, Justice Management Division, U.S. Department of Justice, 1331 Pennsylvania Ave. NW., Suite 1055, Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (i) and add routine use (j) as follows:]

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(j) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

77 FR 5570 (February 3, 2012): Last published in full.

**JUSTICE/DOJ-016**

**SYSTEM NAME AND NUMBER:**

JUSTICE/DOJ-016, Debt Collection Enforcement System.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

The Justice Data Center, Rockville, MD 20854; and the DOJ components and offices throughout the country that have debt collection and enforcement records and/or responsibilities, including the Antitrust Division, the Civil Division, the Civil Rights Division, the Criminal Division, the Justice Management Division (JMD) Debt Collection Management Staff (DCM), the Executive Office for United States Attorneys

(EOUSA), the Environment and Natural Resources Division (ENRD), and the Tax Division. Records may also reside in offices of private counsel retained by DOJ pursuant to contract (contract private counsel) to assist with debt collection.

**SYSTEM MANAGER(S) AND ADDRESS:**

For Debt Collection Management Staff/JMD information contact: FOIA/PA Contact, DOJ/Justice Management Division, 950 Pennsylvania Avenue NW., Room 1111, Washington, DC 20530-0001.

For Antitrust Division information contact: FOIA/PA Unit, DOJ/Antitrust Division, Liberty Square Building, Suite 1000, 450 Fifth Street NW., Washington, DC 20530-0001.

For Civil Division information contact: FOIA/PA Office, DOJ/Civil Division, Room 7304, 20 Massachusetts Avenue NW., Washington, DC 20530-0001.

For Civil Rights Division information contact: FOIA/PA Branch, DOJ/Civil Rights Division, 950 Pennsylvania Avenue NW., BICN, Washington, DC 20530-0001.

For Criminal Division information contact: FOIA/PA Unit, DOJ/Criminal Division, Keeney Building, Suite 1127, Washington, DC 20530-0001.

For Environment and Natural Resources Division information contact: FOIA/PA Office, Law and Policy Section, DOJ/ENRD, P.O. Box 4390, Ben Franklin Station, Washington, DC 20044-4390.

For Executive Office for United States Attorneys (United States Attorneys Offices) information contact: FOIA/PA Staff, DOJ/EOUSA, 600 E Street NW., Room 7300, Washington, DC 20530-0001. Contact information for the individual United States

Attorneys Offices in the 94 Federal judicial districts nationwide can be located at [www.usdoj.gov/usao](http://www.usdoj.gov/usao).

For Tax Division information contact: Assistant Attorney General, Tax Division, U.S. Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (s) as follows:]

(s) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (v) as follows:]

(v) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity

(including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

77 FR 9965 (February 21, 2012): Last published in full; and

80 FR 14407 (March 19, 2012): Modified to add routine uses.

**JUSTICE/DOJ-017**

**SYSTEM NAME AND NUMBER:**

JUSTICE/DOJ-017, Department of Justice, Giglio Information Files.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Records in this system are located at United States Attorneys' Offices and Department of Justice litigating sections with authority to prosecute criminal cases ("DOJ prosecuting offices") as well as the Federal Bureau of Investigation, the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the United States Marshals Service, the Office of the Inspector General, and the Office of Professional Responsibility ("DOJ investigative agencies"). For office locations, see <http://www.justice.gov> and the Web sites for DOJ prosecuting offices and investigative agencies.

**SYSTEM MANAGER(S) AND ADDRESS:**

The system managers for this system are the *Giglio* Requesting Official within each DOJ prosecuting office and the Agency Official within each DOJ investigative

agency, as those officials are defined in Section 9–5.100 of the United States Attorneys’ Manual. For office locations, see [www.justice.gov](http://www.justice.gov) and the Web sites for DOJ prosecuting offices and investigative agencies.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (n) as follows:]

(n) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity

(including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

80 FR 16025 (March 26, 2015): Last published in full.

**JUSTICE/COPS-002**

**SYSTEM NAME AND NUMBER:**

JUSTICE/COPS-002, COPS Online Ordering System.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Records are maintained at two locations where the Community Oriented Policing Services (COPS) Office operations are supported: 145 N Street NE., Washington, DC 20530, and 1151–D Seven Locks Road, Rockville, MD 20854. Contact information is listed on the COPS Internet Web site, <https://www.cops.usdoj.gov/>.

**SYSTEM MANAGER(S) AND ADDRESS:**

Information Technology Operations Manager, COPS Office, 145 N Street NE., Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use D. as follows:]

D. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use J. as follows:]

J. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

77 FR 28898 (May 16, 2012): Last published in full.

**JUSTICE/CRM-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records.

**SECURITY CLASSIFICATION:**

The system itself is, in whole sensitive and in part, classified to protect national security/foreign policy material. Within the unclassified part, items or records may have Limited Official Use or national security/foreign policy classifications.

**SYSTEM LOCATION:**

U.S. Department of Justice, Criminal Division, Washington DC 20530–0001 or a National Archives and Records Administration (NARA) Regional Records Center.

**SYSTEM MANAGER(S) AND ADDRESS:**

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington DC 20530–0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (23) and add routine use (24) as follows:]

(23) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(24) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 44182 (August 7, 2007): Last published in full.

**JUSTICE/CRM-029**

**SYSTEM NAME AND NUMBER:**

JUSTICE/CRM-029, United States Victims of State Sponsored Terrorism Fund (USVSSTF) File System.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Records in this system are located at: U.S. Department of Justice, Criminal Division, 950 Pennsylvania Avenue NW., Washington, DC 20530; Federal Records Center, Suitland, MD 20409, 5151 Blazer Parkway, Suite A, Dublin, OH 43017; and 1985 Marcus Avenue, Suite 200, Lake Success, NY 11042.

**SYSTEM MANAGER(S) AND ADDRESS:**

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 950  
Pennsylvania Avenue NW., Washington, DC 20503-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (i) as follows:]

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (k) as follows:]

(k) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

81 FR 45539 (July 14, 2016): Last published in full.

**JUSTICE/DEA-008**

**SYSTEM NAME AND NUMBER:**

JUSTICE/DEA-008, Investigative Reporting and Filing System.

**SECURITY CLASSIFICATION:**

Classified and unclassified information.

**SYSTEM LOCATION:**

Records in this system are located at the Headquarters Offices of the Drug Enforcement Administration (DEA) in the Washington, DC area, at DEA field offices around the world, at Department of Justice Data Centers, at the DEA Data Center, at secure tape backup storage facilities, and at Federal Records Centers. See [www.dea.gov](http://www.dea.gov) for DEA office locations.

**SYSTEM MANAGER(S) AND ADDRESS:**

Chief of Operations, Operations Division and Assistant Administrator for Intelligence, Intelligence Division, DEA Headquarters, 8701 Morrisette Drive, Springfield, VA 22152.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (j) as follows:]

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (ab) as follows:]

(ab) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

77 FR 21808 (April 11, 2012): Last published in full.

**JUSTICE/FBI-009**

**SYSTEM NAME AND NUMBER:**

JUSTICE/FBI-009, The Next Generation Identification (NGI) System.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Records described in this notice are maintained at the Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division (CJIS), Clarksburg, WV. Some or all system information may be duplicated at other locations, including at FBI facilities, for purposes of system backup, emergency preparedness, and continuity of operations.

**SYSTEM MANAGER(S) AND ADDRESS:**

Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, 1000 Custer Hollow Road, Clarksburg, WV 26306.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use Z. and add routine use AA. as follows as follows:]

Z. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

AA. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

81 FR 27283 (March 5, 2016): Last published in full.

**JUSTICE/FBI-019**

**SYSTEM NAME AND NUMBER:**

JUSTICE/FBI-019, Terrorist Screening Records Center (TSRS).

**SECURITY CLASSIFICATION:**

Classified and unclassified.

**SYSTEM LOCATION:**

Records described in this notice are maintained at the Terrorist Screening Center, Federal Bureau of Investigation, Washington, DC, and at facilities operated by other government entities for terrorism and national security threat screening, system back-up, and continuity of operations purposes.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Terrorist Screening Center, Federal Bureau of Investigation, FBI  
Headquarters, 935 Pennsylvania Avenue NW., Washington, DC 20535-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use L. as follows:]

L. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use N. as follows:]

N. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

76 FR 77846 (December 14, 2011): Last published in full.

**JUSTICE/FBI-020**

**SYSTEM NAME AND NUMBER:**

JUSTICE/FBI-020, Law Enforcement National Data Exchange System (NDEX).

**SECURITY CLASSIFICATION:**

Sensitive But Unclassified.

**SYSTEM LOCATION:**

Records will be located at the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Road, Clarksburg, WV 26306, and at appropriate locations for system backup and continuity of operations purposes.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Federal Bureau of Investigation, 935 Pennsylvania Ave., NW.,  
Washington, DC 20535-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use D. as follows:]

D. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the

Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use F. as follows:]

F. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 56793 (October 4, 2007): Last published in full.

**JUSTICE/FBI-022**

**SYSTEM NAME AND NUMBER:**

JUSTICE/FBI-022, FBI Data Warehouse System.

**SECURITY CLASSIFICATION:**

Classified and/or unclassified information.

**SYSTEM LOCATION:**

Records may be maintained at all locations at which the Federal Bureau of Investigation (FBI) operates or at which FBI operations are supported, including: J. Edgar Hoover Bldg., 935 Pennsylvania Avenue NW., Washington, DC 20535-0001; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Rd., Clarksburg, WV 26306; FBI Records Management Division, 170 Marcel Drive, Winchester, VA 22602-4843; and FBI field offices, legal attaches, information technology centers, and other components as listed on the FBI's Internet Web site, <http://www.fbi.gov>. Some or all system information may also be duplicated at other locations where the FBI has granted direct access for support of FBI missions, for purposes of system backup, emergency preparedness, and/or continuity of operations.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue NW.,  
Washington, DC 20535-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (i.) as follows:]

(i.) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and

operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (z.) as follows:]

(z.) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

77 FR 40630 (July 10, 2012): Last published in full.

**JUSTICE/INTERPOL-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/INTERPOL-001, INTERPOL-United States National Central Bureau (USNCB) Records System.

**SYSTEM LOCATION:**

INTERPOL-U.S. National Central Bureau, Department of Justice, Washington, DC 20530.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530.

Records Management Officer, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530.

Chief Information Officer, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530.

\* \* \* \* \*

**SECURITY CLASSIFICATION:**

[Add security classification as follows:]

Sensitive but Unclassified

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (u) and add routine use (v) as follows:]

(u) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(v) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

75 FR 27821 (May 18, 2010): Last published in full.

**JUSTICE/JMD-003**

**SYSTEM NAME AND NUMBER:**

JUSTICE/JMD-003, Department of Justice Payroll System.

**SYSTEM LOCATION:**

This system of records is managed by the Department of Justice (DOJ), Justice Management Division (JMD), Director, Personnel Staff, Washington, DC 20530. DOJ has contracted with the Department of Agriculture's National Finance Center (NFC) in New Orleans, Louisiana, 70129, to maintain payroll information and conduct payroll-related activities for its employees. Conversion to the NFC began in July of 1991 and was incrementally completed as of May of 1993. Payroll records in electronic or paper format may be found in the following locations:

*a. Post-Conversion Records:* On a computer maintained by the NFC in New Orleans, Louisiana; and at backup facilities in Philadelphia, Pennsylvania. Relevant data may also be stored on Justice Data Center computers or servers at the DOJ for use in

distributing payroll and accounting information to the individual DOJ Bureaus and components. Paper and electronic payroll information may be kept at various time and attendance recording and processing stations around the world. Paper records may be located in the DOJ's Personnel Staff, Washington, DC 20530, in servicing personnel offices throughout the DOJ, and in the offices of employee supervisors and managers.

*b. Pre-Conversion Historical Records:* On magnetic tape at the Justice Data Center in Rockville, Maryland 20854; on microfiche maintained by the DOJ Finance Staff; and in paper format maintained by the DOJ's Finance and Personnel Staffs, servicing personnel offices, and offices of employee supervisors and managers.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Personnel Staff, Justice Management Division, Department of Justice, National Place Building, Room 1110, 1331 Pennsylvania Avenue, NW., Washington, DC 20530.

\* \* \* \* \*

**SECURITY CLASSIFICATION:**

[Add security classification as follows:]

Sensitive But Unclassified.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use G. as follows:]

G. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use T. as follows:]

T. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

69 FR 107 (Jan. 2, 2004): Last published in full.

72 FR 3410 (Jan. 25, 2007): Modified to add a new routine use.

72 FR 51663 (Sept. 10, 2007): Modified to revise existing and add new routine uses.

**JUSTICE/NSD-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/NSD-001, Foreign Intelligence and Counterintelligence Records System.

**SECURITY CLASSIFICATION:**

The majority of information in this system of records is classified. The remaining information is Sensitive But Unclassified.

**SYSTEM LOCATION:**

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

**SYSTEM MANAGER(S) AND ADDRESS:**

Deputy Counsel for Intelligence Policy, Office of Intelligence Policy & Review, National Security Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use J. and add routine use K. as follows:]

J. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 26153 (May 8, 2007): Last published in full.

**JUSTICE/NSD-002**

**SYSTEM NAME AND NUMBER:**

JUSTICE/NSD-002, Registration and Informational Material Files Under the Foreign Agents Registration Act of 1938.

**SECURITY CLASSIFICATION:**

Sensitive but Unclassified.

**SYSTEM LOCATION:**

U.S. Department of Justice; National Security Division; 950 Pennsylvania Ave., NW., Washington, DC 20530.

**SYSTEM MANAGER(S) AND ADDRESS:**

Chief, Foreign Agents Registration Unit, Counterespionage Section, National Security Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise the second to last routine use as follows:]

To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add the below routine use after the last listed routine use as follows:]

To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity

(including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 26156 (May 8, 2007): Last published in full.

**JUSTICE/NSD-003**

**SYSTEM NAME AND NUMBER:**

JUSTICE/NSD-003, Registration Files of Individuals Who Have Knowledge of, or Have Received Instruction or Assignment in, Espionage, Counterespionage, or Sabotage Service or Tactics of a Foreign Government or of a Foreign Political Party.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

U.S. Department of Justice; National Security Division; 950 Pennsylvania Avenue, NW., Washington, DC 20530.

**SYSTEM MANAGER(S) AND ADDRESS:**

Chief, Foreign Agents Registration Unit; Counterespionage Section; National Security Division; U.S. Department of Justice; 950 Pennsylvania Avenue, NW., Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise the second to last routine use as follows:]

To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add the below routine use after the last routine use listed as follows:]

To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 26158 (May 8, 2007): Last published in full.

**JUSTICE/OCDETF-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/OCDETF-001, Organized Crime Drug Enforcement Task Forces  
Management Information System.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

OCDETF Fusion Center, Executive Office for OCDETF, U.S. Department of  
Justice, 1331 Pennsylvania Avenue NW., Suite 1060, Washington, DC 20530. Some or  
all system information may be duplicated at other locations for purposes of system  
backup, emergency preparedness, and continuity of operations.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Executive Office for OCDETF, Department of Justice, 950  
Pennsylvania Avenue NW., Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (t) as follows:]

(t) To appropriate agencies, entities, and persons when (1) the Department  
suspects or has confirmed that there has been a breach of the system of records; (2) the  
Department has determined that as a result of the suspected or confirmed breach there is a  
risk of harm to individuals, DOJ (including its information systems, programs, and  
operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (v) as follows:]

(v) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

78 FR 56737 (September 13, 2013): Last published in full.

**JUSTICE/OCDETF-002**

**SYSTEM NAME AND NUMBER:**

JUSTICE/OCDETF-002, Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System.

**SECURITY CLASSIFICATION:**

Classified and unclassified.

**SYSTEM LOCATION:**

OCDETF Fusion Center, Executive Office for OCDETF, U.S. Department of Justice, 1331 Pennsylvania Avenue NW., Suite 1060, Washington, DC 20530-0001.

Some or all system information may be duplicated at other locations for purposes including system backup, emergency preparedness, and continuity of operations.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, Executive Office for OCDETF, U.S. Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (t) as follows:]

(t) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (v) as follows:]

(v) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing,

minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

78 FR 56926 (September 16, 2013): Last published in full.

**JUSTICE/OIG-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/OIG-001, Office of the Inspector General Investigative Records.

**SECURITY CLASSIFICATION:**

The vast majority of the information in the system is Sensitive but Unclassified. However, there is some classified information as well.

**SYSTEM LOCATION:**

U.S. Department of Justice, Office of the Inspector General (OIG), 950 Pennsylvania Ave., NW., Washington, DC 20530-0001 and 1425 New York Ave., NW., Suites 7100 and 13100, Washington, DC 20530. During the course of an investigation, records are also kept in the investigations field and area offices, the addresses of which are listed on the OIG's Web site at <http://www.usdoj.gov/oig>.

**SYSTEM MANAGER(S) AND ADDRESS:**

Office of the General Counsel, Office of the Inspector General, Department of Justice, 950 Pennsylvania Avenue, NW., Room 4726, Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (q) as follows:]

(q) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (t) as follows:]

(t) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 36725 (July 5, 2007): Last published in full.

**JUSTICE/OPA-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/OPA-001, Executive Clemency Case Files/Executive Clemency Tracking System.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Office of the Pardon Attorney (OPA), U.S. Department of Justice, Washington, DC 20530.

**SYSTEM MANAGER(S) AND ADDRESS:**

Pardon Attorney, Office of the Pardon Attorney, U.S. Department of Justice, Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (m) as follows:]

(m) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

\* \* \* \* \*

[Add routine use (o) as follows:]

(o) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

76 FR 57078 (September 15, 2011): Last published in full.

**JUSTICE/OPR-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/OPR-001, Office of Professional Responsibility Record Index.

**SECURITY CLASSIFICATION:**

Unclassified Information and Classified Information.

**SYSTEM LOCATION:**

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington,  
DC 20530-0001

**SYSTEM MANAGER(S) AND ADDRESS:**

Counsel, Office of Professional Responsibility, Department of Justice, 950  
Pennsylvania Avenue, NW., Room 3525, Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (18) and add routine use (19) as follows:]

(18) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(19) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

76 FR 66752 (October 27, 2011): Last published in full.

**JUSTICE/OVW-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/OVW-001, Peer Reviewer Database.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Office on Violence Against Women, 145 N Street NE., Suite 10W121, Washington, DC 20530. Duplicate information may be stored at other locations for purposes of system backup, emergency preparedness, and continuity of operations.

**SYSTEM MANAGER(S) AND ADDRESS:**

Acquisition Liaison Specialist, Office on Violence Against Women, 145 N Street NE., Suite 10W121, Washington, DC 20530.

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (f) and add routine use (g) as follows:]

(f) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and

operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(g) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

79 FR 28774 (May 19, 2014): Last published in full.

**JUSTICE/USM-001**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-001, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (k) and add routine use (l) as follows:]

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(l) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 516 (June 18, 2007): Last published in full.

**JUSTICE/USM-002**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-002, Internal Affairs System.

**SECURITY CLASSIFICATION:**

Limited Official Use.

**SYSTEM LOCATION:**

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

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) and add routine use (m) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(m) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 517 (June 18, 2007): Last published in full.

**JUSTICE/USM-004**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-004, Special Deputation Files.

**SECURITY CLASSIFICATION:**

Limited Official Use.

**SYSTEM LOCATION:**

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

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) and add routine use (m) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(m) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 518 (June 18, 2007): Last published in full.

**JUSTICE/USM-005**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-005, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) and add routine use (m) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(m) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 519 (June 18, 2007): Last published in full.

**JUSTICE/USM-006**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-006, 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>).

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (k) and add routine use (l) as follows:]

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(l) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 522 (June 18, 2007): Last published in full.

**JUSTICE/USM-007**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-007, Warrant Information Network (WIN).

**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>.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) and add routine use (m) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(m) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient

agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 9777 (March 5, 2007): Last published in full.

**JUSTICE/USM-008**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-008, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (j) and add routine use (k) as follows:]

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(k) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 523 (June 18, 2007): Last published in full.

**JUSTICE/USM-009**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-009, 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>*.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) and add routine use (m) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department  
suspects or has confirmed that there has been a breach of the system of records; (2) the  
Department has determined that as a result of the suspected or confirmed breach there is a  
risk of harm to individuals, DOJ (including its information systems, programs, and  
operations), the Federal Government, or national security; 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 breach or to prevent,  
minimize, or remedy such harm.

(m) To another Federal agency or Federal entity, when the Department determines  
that information from this system of records is reasonably necessary to assist the recipient

agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 524 (June 18, 2007): Last published in full.

**JUSTICE/USM-010**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-010, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (k) and add routine use (l) as follows:]

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(l) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 526 (June 18, 2007): Last published in full.

**JUSTICE/USM-011**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-011, 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>.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (j) and add routine use (k) as follows:]

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(k) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient

agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 527 (June 18, 2007): Last published in full.

**JUSTICE/USM-013**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-013, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (l) and add routine use (m) as follows:]

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(m) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 529 (June 18, 2007): Last published in full.

**JUSTICE/USM-016**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-016, U.S. Marshals 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (i) and add routine use (j) as follows:]

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(j) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 530 (June 18, 2007): Last published in full.

**JUSTICE/USM-017**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-017, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (i) and add routine use (j) as follows:]

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(j) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 531 (June 18, 2007): Last published in full.

**JUSTICE/USM-018**

**SYSTEM NAME AND NUMBER:**

JUSTICE/USM-018, 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.

**SYSTEM MANAGER(S) AND ADDRESS:**

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

\* \* \* \* \*

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

\* \* \* \* \*

[Revise routine use (k) and add routine use (l) as follows:]

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

(l) To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient

agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

**HISTORY:**

72 FR 33515, 532 (June 18, 2007): Last published in full.

[FR Doc. 2017-10781 Filed: 5/24/2017 8:45 am; Publication Date: 5/25/2017]