

the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure pursuant to 5 U.S.C. 552a(b)(12). Disclosures may be made from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Act of 1966 (31 U.S.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper records are contained in file folders stored within filing cabinets. Electronic records are maintained in computers, computer databases, email, and electronic media such as removable hard drives, magnetic disks, compact discs, and computer tapes.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records in the system are retrieved by permittee's name, permit number or date of activity.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained in accordance with the NPS Service Records Schedule Resource Management and Lands (Category 1). This schedule has been approved by NARA (Job No. N1-79-08-1). The disposition is temporary. Retention of records with short-term operational value and not considered essential for the ongoing management of land and cultural and natural resources are destroyed 15 years after closure. Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 384 Departmental Manual 1.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security rules and policies. Paper records are maintained in file cabinets located in secured DOI facilities under the control of authorized personnel.

Access to DOI networks and records in this system requires DOI credentials or a valid username, password and is limited to DOI personnel who have a need to know the information for the

performance of their official duties. Computers and storage media are encrypted in accordance with DOI security policy. Computers containing files are password protected to restrict unauthorized access. The computer servers in which electronic records are stored are located in secured DOI facilities.

Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974, as amended, 5 U.S.C. 552a; Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.*; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 *et seq.*; and the Federal Information Processing Standards 199: Standards for Security Categorization of Federal Information and Information Systems. Security controls include user identification, passwords, database permissions, encryption, firewalls, audit logs, and network system security monitoring, and software controls.

Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

RECORD ACCESS PROCEDURES:

An individual requesting records on himself or herself should send a signed, written inquiry to the applicable System Manager identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES:

An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the applicable System Manager as identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the applicable System Manager as identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. The request envelope and letter should both be clearly marked "PRIVACY ACT INQUIRY." A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

79 FR 9272 (February 18, 2014).

Teri Barnett,

Departmental Privacy Officer, Department of the Interior.

[FR Doc. 2021-14985 Filed 7-13-21; 8:45 am]

BILLING CODE 4312-52-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 006-2020]

Privacy Act of 1974; Systems of Records

AGENCY: Office of Legal Policy, United States Department of Justice.

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, as amended, and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Office of Legal Policy (OLP), a component within the United States Department of Justice (DOJ or Department), proposes to modify its system of records notice titled "General Files System of the Office of Legal Policy," JUSTICE/OLP-003. OLP proposes to modify this system of records notice as part of the Department's overall effort to update leadership system of records notices in light of organizational, procedural, and technological changes at the Department.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), the modifications to this system of records will be effective upon publication, subject to a 30-day period in which to comment on the modified routine uses, described below. Please submit any comments by August 13, 2021.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments by mail to the United States Department of Justice, Office of Privacy

and Civil Liberties, ATTN: Privacy Analyst, Two Constitution Square (2Con), 145 N Street NE, Suite 8W.300, Washington, DC 20530; by facsimile at 202-307-0693; or by email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Matrina Matthews, Executive Officer, Office of Legal Policy, U.S. Department of Justice, 950 Pennsylvania Avenue NW, Room 4234, Washington, DC 20530-0001; telephone: (202) 616-0040.

SUPPLEMENTARY INFORMATION: OLP is principally responsible for planning, developing, and coordinating the implementation of major policy initiatives of high priority to the Department and to the Administration. In addition, the Assistant Attorney General, OLP, consistent with 28 CFR 0.23, is responsible for: Examining and studying legislation and other policy proposals and coordinating Departmental efforts to secure enactment of those of special interest to the Department and the Administration; advising and assisting the Attorney General and the Deputy Attorney General regarding the selection and appointment of Federal judges; representing the Department on the Administrative Conference of the United States and, as appropriate, on regulatory reform matters; advising appropriate Departmental officials, from time to time, on investigation, litigation, negotiation, penal, or correctional policies to ensure the compatibility of those policies with overall Departmental goals; and performing such other duties and functions as may be specially assigned by the Attorney General and the Deputy Attorney General.

The Department established the system of records, "General Files System of the Office of Legal Policy," JUSTICE/OLP-003, to assist the Assistant Attorney General, OLP, and the personnel within OLP in carrying out the responsibilities of the Office. Since JUSTICE/OLP-003 was last published in full, 50 FR 37299 (Sept. 12, 1985), OLP and the Department as a whole have undertaken a number of organizational, procedural, and technological changes that have modernized the information and information system that are used to collect, use, maintain, and disseminate these records.

Specifically, JUSTICE/OLP-003 is being updated as follows: The system location paragraph has been updated to account for the location of both hard copies and the Department's data

centers; the authorities paragraph has been clarified to include statutes outlining the role and responsibilities of the Assistant Attorney General and OLP, as delegated by the Attorney General; the routine uses have been updated to include additional routine uses that appear in almost every DOJ system of records notice, which allow for disclosures that are functionally equivalent to the purpose for which the DOJ information is collected, or are necessary and proper uses of the DOJ information (for example, disclosures to NARA, disclosure to identify and mitigate actual or suspected breaches, and disclosures to the public or news media, when appropriate); the records-storage paragraph has been updated to include the electronic storage of records; the paragraph detailing the policies and practices for the retrieval of records in the system has been updated to account for the electronic storage of records; the records-retention paragraph has been updated to include the appropriate records control schedules; the access, amendment, and notification procedures have been clarified to detail the process for requesting access to, amendment of, or notification of, records within this system of records not otherwise exempt from such requests; and a history paragraph has been added. The Department has not amended the Privacy Act exemptions already claimed for this system of records, so that paragraph remains unchanged. The Department has published this system of records in its entirety for the benefit of the public.

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

Dated: July 1, 2021.

Peter A. Winn,
Acting Chief Privacy and Civil Liberties Officer, United States Department of Justice.

JUSTICE/OLP-003

SYSTEM NAME AND NUMBER:

General Files System of the Office of Legal Policy, JUSTICE/OLP-003.

SECURITY CLASSIFICATION:

Classified and Controlled Unclassified Information.

SYSTEM LOCATION:

Hard-copy records will be maintained at OLP, Robert F. Kennedy Department of Justice Building, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001.

Electronic records will be maintained at one or more of the Department's data centers, including, but not limited to,

the Justice Data Center, Rockville, MD 20854, and/or at one or more of the Department's Core Enterprise Facilities (CEF), including, but not limited to, the Department's CEF East, Clarksburg, WV 26306, or CEF West, Pocatello, ID 83201. Records within this system of records may be transferred to a Department-authorized cloud service provider, in which records would be limited to locations within the continental United States. Access to these electronic records includes all locations at which OLP operates or at which OLP operations are supported, including the Robert F. Kennedy Department of Justice Building. Some or all system information may also be duplicated at other locations where the Department has granted direct access to support OLP operations, system backup, emergency preparedness, and/or continuity of operations.

To determine the location of particular OLP records, contact the system manager, whose contact information is listed in the "SYSTEM MANAGER(S)" paragraph, below.

SYSTEM MANAGER(S):

Assistant Attorney General, Office of Legal Policy, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001; phone: 202-514-4601; general inquiries to the Department can be submitted online at: <https://www.justice.gov/contact-us>.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

These records are maintained pursuant to 28 U.S.C. ch. 31; 5 U.S.C. 301; and 28 CFR part 0, subpart D-2.

PURPOSE(S) OF THE SYSTEM:

This system is maintained for the purpose of assisting the Assistant Attorney General, OLP, in carrying out OLP's responsibilities. OLP is principally responsible for planning, developing, and coordinating the implementation of major policy initiatives of high priority to the Department and to the Administration. In addition, the Assistant Attorney General, OLP, consistent with 28 CFR 0.23: Examines and studies legislation and other policy proposals and coordinates Departmental efforts to secure enactment of those of special interest to the Department and the Administration; advises and assists the Attorney General and the Deputy Attorney General regarding the selection and appointment of Federal judges; represents the Department on the Administrative Conference of the United States and, as appropriate, on regulatory reform matters; advises appropriate Departmental officials, from

time to time, on investigation, litigation, negotiation, penal, or correctional policies to ensure the compatibility of those policies with overall Departmental goals; and performs such other duties and functions as may be specially assigned by the Attorney General and the Deputy Attorney General.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system may encompass individuals who are involved with official Federal investigations, policy decisions, and administrative matters of significance. Such individuals include, but are not limited to, subjects of litigation, targets of investigations, Members and staff members of Congress, government officials, and individuals of national prominence or notoriety. The system also encompasses individuals who were candidates for Federal judgeships but who were never nominated, individuals who were nominated for Federal judgeships but who were never confirmed, and individuals who were nominated and confirmed for Federal judgeships, excluding those appointed to the United States Court of Appeals for the Armed Forces, the United States Court of Appeals for Veterans Claims, the United States Tax Court, and the United States Court of Military Commission Review. The Assistant Attorney General, OLP, maintains records indexed to the name of the individual.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include case files, litigation materials, exhibits, internal memoranda and reports, or other records on a given subject or individual. Records vary in number and kind according to the breadth of the responsibilities assigned to the Assistant Attorney General, OLP. Records include those of such significance that the Assistant Attorney General, OLP, has policy or administrative interest, and may include those which pertain to investigative or law enforcement cases for which the Assistant Attorney General, OLP, is asked to provide an analysis and establish future policy direction. A computerized index containing the subject title and/or individual's name is also maintained.

RECORD SOURCE CATEGORIES:

Sources of information contained in this system not otherwise exempt include individuals; organizations; State, local, and foreign government agencies as appropriate; the executive and legislative branches of the Federal Government; relevant third parties, and other Department and OLP systems of

records, including but not limited to, JUSTICE/OLP-002, Judicial Nominations Files.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system of records may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

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

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

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

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

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

(F) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would

constitute an unwarranted invasion of personal privacy.

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

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

(I) To Federal, State, local, territorial, tribal, foreign, or international licensing agencies or associations that require information concerning the suitability or eligibility of an individual for a license or permit.

(J) To a Member of Congress, or staff acting upon the Member's behalf, when the Member or staff requests the information for investigative or policy decision-making purposes, or on behalf of, or at the request of, the individual who is the subject of the record.

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

(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, the Department (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.

(N) To any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of OLP and meeting related reporting requirements.

(O) To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

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

(Q) To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for such purposes.

(R) To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such threat.

(S) To any person or entity if deemed by OLP to be necessary in order to elicit information or cooperation from the recipient for use by OLP in the performance of an authorized law enforcement activity.

(T) To officials and employees of the White House, and during Presidential transitions, the President-elect and Vice President-elect and their designees, or any Federal agency which requires information relevant to an agency concerning the hiring, appointment, or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation, the classifying of a job, or the issuance of a grant or benefit.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system may be stored in electronic form, stored in paper folders, and/or stored on magnetic disks, hard disks, removable storage devices, or other electronic media. Electronic records are stored in databases and/or on hard disks, removable storage devices, or other electronic media. Records are stored securely in accordance with applicable executive orders, statutes, and agency implementing recommendations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved manually by personal identifier (e.g., name of the

individual, registration number, employee identification number, etc.); subject title; or in some cases, by other identifying search terms.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with guidelines approved by the National Archives and Records Administration (DAA-006-2013-0005 (pending), DAA-0060-2012-0009, and DAA-006-2016-0006 (pending)).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information in this system is maintained in accordance with applicable laws, rules, and policies on protecting individual privacy. The servers storing electronic data and the backup tapes stored onsite are located in locked rooms with access limited to authorized agency personnel. Backup tapes stored offsite are maintained in accordance with a government contract that requires adherence to applicable laws, rules, and policies on protecting individual privacy. Internet connections are protected by multiple firewalls. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance, and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations. Users of individual computers can only gain access to the data with a valid user identification and password.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the Chief, Initial Request Staff, Office of Information Policy, 1425 New York Avenue NW, Suite 11050, Washington, DC 20530-0001. Requests may also be made online at <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. The envelope, letter, and/or subject line should be clearly marked "Privacy Act Access Request." The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort in accordance with 28 CFR 16.41(d). The request must include a general description of the records sought and must include the requester's full name, current address, and, when necessary to identify records, date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Some information may be exempt from the access provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An

individual who is the subject of a record in this system of records may request access to those records that are not exempt from access. A determination of whether a record may be accessed will be made at the time a request is received.

Although no specific form is required to submit a request, you may obtain forms for this purpose from the FOIA/Privacy Act Mail Referral Unit, United States Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, or on the Department of Justice website at <https://www.justice.gov/oip/make-foia-request-doj>.

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR part 16 Subpart D, "Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "RECORD ACCESS PROCEDURES" paragraph, above. All requests to contest or amend records must be in writing, and the envelope, letter, and/or subject line should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reason(s) for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system of records may request to contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

More information regarding the Department's procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR 16.46, "Requests for Amendment or Correction of Records."

NOTIFICATION PROCEDURES:

Individuals may request to be notified if a record in this system of records pertains to them by utilizing the same procedures identified in the "RECORD ACCESS PROCEDURES" paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and

(4); (d); (e)(1), (2), and (3), (e)(4)(G) and (H), and (e)(5); and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the **Federal Register**.

HISTORY:

50 FR 37299 (Sept. 12, 1985): Last published in full;

66 FR 8425 (Jan. 31, 2001): Added one routine use;

72 FR 3410 (Jan. 25, 2007): Added one routine use; and

82 FR 24147 (May 25, 2017): Rescinded 72 FR 3410, and added two routine uses.

[FR Doc. 2021-14994 Filed 7-13-21; 8:45 am]

BILLING CODE P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 002-2021]

Privacy Act of 1974; Systems of Records

AGENCY: United States Department of Justice.

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a, and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Department of Justice (Department or DOJ), proposes to modify an existing DOJ system of records previously titled, “Department of Justice Computer Systems Activity and Access Records,” JUSTICE/DOJ-002. The Department proposes to modify JUSTICE/DOJ-002 to reflect changes in technology, including the increased ability of the Department to link individuals to information technology, information system, or network activity, and to better describe the Department’s records linking individuals to reported cybersecurity incidents or their access to certain DOJ information technologies, information systems, and networks through the internet or other authorized connections.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by August 13, 2021.

ADDRESSES: The public, Office of Management and Budget (OMB), and Congress are invited to submit any

comments by mail to the Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, 145 N St. NE, Suite 8W.300, Washington, DC 20530, by facsimile at 202-307-0693, or by email to privacy.compliance@usdoj.gov.

FOR FURTHER INFORMATION CONTACT:

Nickolous Ward, DOJ Chief Information Security Officer, (202) 514-3101, 145 N Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION:

In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, DOJ is responsible for complying with information security policies and procedures requiring information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. *See, e.g.*, 44 U.S.C. 3554 (2018). Consistent with these requirements, DOJ must ensure that it maintains accurate audit and activity records of the observable occurrences on its information systems and networks (also referred to as “events”) that are significant and relevant to the security of DOJ information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Additionally, monitored events—whether detected utilizing information systems maintaining audit and activity records, reported to the Department by information system users, or reported to the Department by the cybersecurity research community and members of the general public conducting good faith vulnerability discovery activities—may constitute occurrences that (1) actually or imminently jeopardize, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The Department has developed a formal process to track and document these reported “incidents,” which may, in limited circumstances, include records of individuals reporting, or otherwise associated with, an actual or suspected event or incident.

The system of records previously titled JUSTICE/DOJ-002, “Computer Systems Activity and Access Records,” covers the Department’s tracking of all DOJ information technology, information system, and/or network activity, including any access, whether authorized or unauthorized, by users to any DOJ information technology, DOJ information systems, and/or DOJ networks. These records assist Department information security professionals in protecting DOJ data, ensuring the secure operation of DOJ information systems, and tracking and documenting incidents reported to the Department. JUSTICE/DOJ-002 was first published at 64 FR 73,585, on December 30, 1999, and later modified at 66 FR 8,425, on January 31, 2001, and 82 FR 24,147, on May 25, 2017. The revisions to this notice reflect advances in technology, such as the ability of authorized users to connect to Department information systems through the internet or other authorized network connections, as well as the increased ability of the Department to link the identity of individuals or subjects associated with an actual or suspected event or incident for security and administrative purposes.

The Department proposes to modify JUSTICE/DOJ-002 by: Revising the title of the system of records to, “Department of Justice Information Technology, Information System, and Network Activity and Access Records;” modifying and clarifying the location of the system’s records; clarifying the individuals covered by the system to include any and all individuals who access Department information systems for any reason and from any location; clarifying the way in which the records maintained in this system of records are retrieved; expanding the routine uses of records for disclosures that are functionally equivalent to the purpose for which the DOJ information is collected, or that are necessary and proper uses of the DOJ information, to enhance the flexibility of JUSTICE/DOJ-002; and to notify the public that the Department intends to claim certain Privacy Act exemptions, promulgated elsewhere in the **Federal Register**. DOJ is republishing the entire system of records notice for ease of reference to these changes.

In accordance with Privacy Act requirements of 5 U.S.C. 552a(r), the Department has provided a report to OMB and to Congress on this revised system of records.