may also be obtained by accessing its internet server at *https://www.usitc.gov.* The public record for this investigation may be viewed on the Commission's electronic docket (EDIS) at *https://edis.usitc.gov.* Hearing-impaired persons are advised that information on this matter can be obtained by contacting the Commission TDD terminal on (202) 205–1810.

SUPPLEMENTARY INFORMATION: The Commission instituted this investigation on January 22, 2018, based upon an amended and supplemented complaint filed by Lakshmi Arunachalam, Ph.D. and WebXchange, Inc., both of Menlo Park, California. 83 FR 3021 (Jan. 22, 2018). The complaint alleged violations of section 337 of the Tariff Act of 1930, as amended (19 U.S.C. 1337), by a number of proposed respondents in the importation into the United States, the sale for importation, or the sale within the United States after importation of certain IOT devices and components thereof (IOT, the Internet of Things)—web applications displayed on a web browser by reason of infringement of certain claims of U.S. Patent No. 7,930,340 (''the '340 patent''), as well as unfair methods of competition and unfair acts (criminal and civil RICO violations, breach of contract, theft of intellectual property, antitrust violations, and trade secret misappropriation), the threat or effect of which is to destroy or substantially injure an industry in the United States. 83 FR at 3021. The Commission determined to institute the investigation only as to infringement of the '340 patent, and named as respondents Apple Inc. of Cupertino, California; Facebook, Inc. of Menlo Park, California; Samsung Electronics America, Inc. of Ridgefield Park, New Jersey; and Samsung Electronics Co., Ltd. of Seoul, South Korea. *Id.* at 3022. The Office of Unfair Import Investigations (''OUII'') was also named as a party. *Id.*

On January 29, 2018, the respondents moved to terminate the investigation based upon the then-imminent expiration of the '340 patent. The complainants responded in opposition to the motion. The ALJ denied the motion for failure to comply with Commission rules. Order No. 8 at 2 & n.1 (Feb. 20, 2018). On February 21, 2018, the respondents filed a renewed motion to terminate, which corrected the omission in their previous motion. The complainants renewed their opposition to the motion. OUII supported the motion.

On February 27, 2018, the ALJ granted the motion as an ID, finding that good cause exists for terminating the investigation. The ID finds that given ''the structure of section 337 investigations'' there was insufficient time for the Commission to ''reach a final determination or issue any relief before the March 5, 2018 expiration date'' of the '340 patent. Order No. 10 at 6.

On March 5, 2018, the '340 patent expired. That same day, the complainants filed a ''Motion for Rehearing and Reinstating the Investigation'' (''Compl'ts Submission''). The Commission determined to treat that submission as a petition for Commission review of the ID under 19 CFR 210.43. The petition seeks an advisory ruling on certain issues. Compl'ts Submission 6.

On March 12, 2018, the respondents and OUII filed responses in opposition to the complainants' submission. The responses explain, *inter alia,* that the complainants' submission does not provide an adequate basis for Commission review under Commission Rule 210.43(b)(1), 19 CFR 210.43(b)(1). Resp'ts Resp. 3; OUII Resp. 1, 3.

Having considered the record of the investigation, including the parties' submissions to the Commission, the Commission decides as follows. The Commission ''can issue only an exclusion order barring future importation or a cease and desist order barring future conduct,'' neither of which can issue as to an expired patent. *Texas Instruments Inc.* v. *U.S. Int'l Trade Comm'n,* 851 F.2d 342, 344 (Fed. Cir. 1988). Because the'340 patent has now actually expired, the ID's good cause (the imminent expiration of the patent) is now moot. Accordingly, the Commission has determined to review the ID, and, on review, to affirm the termination based upon the actual expiration of the '340 patent. The Commission declines the complainants' invitation to issue advisory rulings, and terminates the investigation.

The authority for the Commission's determination is contained in section 337 of the Tariff Act of 1930, as amended (19 U.S.C. 1337), and in part 210 of the Commission's Rules of Practice and Procedure (19 CFR part 210).

By order of the Commission.

Issued: March 23, 2018.

Katherine M. Hiner,

Supervisory Attorney.

[FR Doc. 2018–06220 Filed 3–27–18; 8:45 am]

BILLING CODE 7020–02–P

JUDICIAL CONFERENCE OF THE UNITED STATES

Meeting of The Judicial Conference; Committee on Rules of Practice and Procedure

AGENCY: Judicial Conference of the United States, Committee on Rules of Practice and Procedure.

ACTION: Notice of open meeting.

SUMMARY: The Committee on Rules of Practice and Procedure will hold a meeting on June 12, 2018. The meeting will be open to public observation but not participation. An agenda and supporting materials will be posted at least 7 days in advance of the meeting at: *http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books.*

DATES: June 12, 2018.

Time: 8:30 a.m. to 5:00 p.m.

ADDRESSES: Thurgood Marshall Federal Judiciary Building, Mecham Conference Center, Administrative Office of the United States Courts, One Columbus Circle NE, Washington, DC 20544.

FOR FURTHER INFORMATION CONTACT: Rebecca A. Womeldorf, Rules Committee Secretary, Rules Committee Staff, Administrative Office of the United States Courts, Washington, DC 20544, telephone (202) 502–1820.

Dated: March 22, 2018.

Rebecca A. Womeldorf,

Rules Committee Secretary.

[FR Doc. 2018–06157 Filed 3–27–18; 8:45 am]

BILLING CODE 2210–55–P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 004–2018]

Privacy Act of 1974; Systems of Records

AGENCY: National Institute of Justice, Office of Justice Programs, United States Department of Justice.

ACTION: Notice of a new system 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 Office of Justice Programs (hereinafter OJP), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records titled National Missing and Unidentified Persons System, JUSTICE/OJP—015. The OJP proposes to establish this system of records to improve the quantity and quality of—and appropriate access to—

data on missing persons, unidentified decedents, and unclaimed decedents, in a centralized repository.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is applicable upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by April 27, 2018.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, National Place Building, 1331 Pennsylvania Avenue NW, Suite 1000, Washington, DC 20530, or 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.

FOR FURTHER INFORMATION CONTACT: Charles Heurich, Senior Physical Scientist, National Institute of Justice, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, *Charles.Heurich@usdoj.gov,* 202–616–9264.

SUPPLEMENTARY INFORMATION: The National Institute of Justice's National Missing and Unidentified Persons System (NamUs) houses records and information in a centralized system regarding cases of missing persons, unidentified persons (decedents), and unclaimed persons (decedents), and makes certain information available, based on access privileges, to the general public, law enforcement professionals, coroners, and medical examiners to help solve such cases. 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: March 16, 2018.

Katherine M. Harman-Stokes,

Deputy Director, Office of Privacy and Civil Liberties, United States Department of Justice.

SYSTEM NAME AND NUMBER

National Missing and Unidentified Persons System (NamUs), JUSTICE/OJP—015

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Office of Justice Programs, 810 7th Street NW, Washington, DC 20531

SYSTEM MANAGER(S):

Point of Contact: Charles Heurich, *Charles.Heurich@usdoj.gov,* National Institute of Justice, Office of Investigative and Forensic Sciences, 810 7th Street NW, Washington, DC 20531

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title I of the Omnibus Crime Control and Safe Streets Act of 1968 (sections 201 and 202); Homeland Security Act of 2002 (section 232); and 28 U.S.C. 530C.

PURPOSE(S) OF THE SYSTEM:

The National Missing and Unidentified Persons System (NamUs) houses records and information regarding cases of missing persons, unidentified decedents, and unclaimed decedents, and makes appropriate information available to the general public and law enforcement professionals to help solve such cases.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Missing persons and registered users of the system, including registered law enforcement personnel, coroners, medical examiners, and members of the public, and although not covered by the Privacy Act, unidentified decedents and unclaimed decedents (named but no next of kin).

CATEGORIES OF RECORDS IN THE SYSTEM:

Missing person case information, unidentified decedent case information, unclaimed decedent case information, and administrative data for registered users. Case information that is available to the general public may include, but is not limited to, case numbers, name, demographic information (such as age, gender, race/ethnicity, height, and weight), last known location, date of last contact, physical description, clothing and accessories, vehicle and transportation information, investigating agency information, and photographs. Professional users have access to additional case information that may include, but is not limited to, date of birth, place of birth, Social Security number (SSN) (for missing persons cases only), DNA availability (specifically whether a DNA sample exists and was submitted to a laboratory, and if so, which laboratory and whether the lab results are available—neither DNA profiles nor DNA testing results are housed within the NamUs system), fingerprint records, dental records, and family contact information. Administrative data for registered users includes, but is not limited to, name, address, email address, telephone number, work title (for professional users only) and agency name (for professional users only).

RECORD SOURCE CATEGORIES:

Professional users and members of the public provide information for the system:

- *Professional Users:* Law Enforcement, Medical Examiners/Forensic Pathologists, Coroners, Medicolegal Investigators, DNA Specialists, Fingerprint Examiners, Forensic Odontologists, Forensic Anthropologists, Regional System Administrators (OJP grantees), NamUs Staff (*i.e.* staff that do not have the ability to grant access to other users or have final approval over edits or changes), and National Center for Missing and Exploited Children (NCMEC) Liaisons.
- *Public Users:* members of public including family members of missing persons, victim advocates, media representatives, and other members of the public who have registered as users in the NamUs application.

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:

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

2. To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, medicolegal, or national security intelligence information for such purposes when determined to be relevant by the DOJ.

3. 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.

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

5. 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.

6. To the news media and members of the general public, 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.

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

8. To designated officers and employees of federal, state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

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

10. To former employees of the Department for purposes of: Responding to an official inquiry by a federal, state, local, tribal or territorial government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with former employees 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.

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

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

13. 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.

14. 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 efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

15. 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.

16. To any agency, organization, or individual for the purposes of performing authorized audit and oversight operations of the DOJ and meeting related reporting requirements.

17. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored in electronic form for use in a computer environment.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information in this system may be retrieved by personal identifier, including but not limited to, an individual's name, case number, physical description, and other unique case information metadata, such as scars, marks, and tattoos.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records will be maintained in a secure manner within the NamUs information technology system until disposition. The retention period for the NamUs system is pending; until the National Archives and Records Administration approves the retention and disposal schedule, records will be treated as permanent.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Internet connections are protected by multiple firewalls. Information technology security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all DOJ computers that access the system to assist in troubleshooting and forensic analysis during incident investigations. For access to sensitive information that is not published for public access, users of the system can only gain access to the data based on their access privileges and by a valid user identification and password. Access to the data in the system is further limited by the user's assigned role within the system. All communications between users and the system are protected by secure communication protocol that provides confidentiality and integrity of the transmitted data. The system leverages Federal Risk and Authorization Management Program (FedRAMP) compliant cloud service infrastructure with security controls including physical safeguards appropriate for a system categorized as ''moderate'' under applicable Federal Information Security Modernization Act of 2014 (FISMA)-related information technology standards.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the Government Information Specialist, Office of Justice Programs, Department of Justice, Room 5400, 810 7th Street NW, Washington, DC 20531 or *FOIAOJP@usdoj.gov.* The envelope and letter 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. The request must include a general

description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Although no specific form is required, 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 *http://www.justice.gov/oip/oip-request.html.*

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 section, above. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked ''Privacy Act Amendment Request.'' All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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 be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the RECORD ACCESS PROCEDURES section, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2018–05971 Filed 3–27–18; 8:45 am]

BILLING CODE 4410–18–P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 002–2018]

Privacy Act of 1974; Systems of Records

AGENCY: Office of Inspector General, United States Department of Justice.

ACTION: Notice of a new system 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 Office of Inspector General (OIG), a component within the United States Department of Justice (DOJ or Department), is publishing a new system of records notice titled ''Data Analytics Program Records System,'' JUSTICE/OIG–006. OIG proposes to establish this system of records to assist with the performance of audits, investigations, and reviews, and to accommodate the requirements of the Digital Accountability and Transparency Act of 2014 (DATA Act).

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is applicable upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Therefore, please submit any comments by April 27, 2018.

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, National Place Building, 1331 Pennsylvania Avenue NW, Suite 1000, 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: William Blier, General Counsel, Office of the General Counsel, Office of the Inspector General, Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, (202) 514–3435.

SUPPLEMENTARY INFORMATION: Under the Inspector General Act of 1978, as amended, Inspectors General, including the DOJ Inspector General, are responsible for conducting, supervising, and coordinating audits and investigations relating to programs and operations of the Federal agency for which their office is established to recognize and mitigate fraud, waste, and abuse. This system of records facilitates OIG's performance of its statutory responsibility by implementing a data analytics (DA) program to assist with the performance of OIG audits, investigations, and reviews, and accommodate the requirements of the DATA Act, Public Law 113–101, 128 Stat. 1146.

The DA program will provide OIG: Timely insights from the data already stored in DOJ databases that OIG has legal authorization to access and maintain; the ability to monitor and analyze data for patterns and correlations that signal wasteful, fraudulent, or abusive activities impacting Department performance and operations; the ability to find, acquire, extract, manipulate, analyze, connect, and visualize data; the capability to manage vast amounts of data; the ability to identify significant information that can improve decision quality; and the ability to mitigate risk of waste, fraud, and abuse. The DA program will also allow the OIG to obtain technology to develop risk indicators that can analyze large volumes of data and help focus OIG's efforts to combat waste, fraud, and abuse. OIG intends to use statistical and mathematical techniques to identify areas to conduct audits and identify activities that may indicate whether an investigation is warranted. The information maintained within this system of records will be limited to only information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs and operations to recognize and mitigate fraud, waste, and abuse.

Pursuant to 5 U.S.C. 552a(b)(12), records maintained in this system of records may be disclosed to a consumer reporting agency without the prior written consent of the individual to whom the record pertains. Such disclosure will only be made in accordance 31 U.S.C. 3711(e). 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: March 15, 2018.

Katherine Harman-Stokes,

Deputy Director, Office of Privacy and Civil Liberties, United States Department of Justice.

JUSTICE/OIG–006

SYSTEM NAME AND NUMBER:

Data Analytics Program Records System, JUSTICE/OIG–006.

SECURITY CLASSIFICATION:

Classified and Controlled Unclassified Information.

SYSTEM LOCATION:

Access to these electronic records includes all Department locations that the Department's Office of Inspector General (OIG) operates or that support OIG operations, including but not limited to, 1425 New York Avenue, Washington, DC 20005. Some or all system information may also be duplicated at other locations where the Department has granted direct access to