Dated: June 15, 2022.

Angelia Rorison,

USCCR Media and Communications Director.

[FR Doc. 2022–13201 Filed 6–15–22; 11:15 am]

BILLING CODE 6335–01–P

DEPARTMENT OF COMMERCE

[Docket No. 2203290081]

Privacy Act of 1974; System of Records

AGENCY: Office of the Inspector General, Department of Commerce.

ACTION: Notice of a new system of records.

SUMMARY: This notice announces the Department of Commerce's (the Department) proposal to establish a new system of records entitled ''COMMERCE/OIG–2, OIG Data Analytics Records,'' under the Privacy Act of 1974, as amended, and the Office of Management and Budget (OMB) Circular A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.'' This system of records will store individually identifying information gathered or created from existing systems of records maintained by the Department, other Department records, and private sources regarding or supporting Department operations. The new system will be used, primarily through data analytics techniques, to identify suspicious or fraudulent activity, internal control weaknesses, or otherwise to assist the Office of Inspector General (OIG) in the performance of its statutory duties under the Inspector General Act of 1978, as amended. We invite public comment on the new system announced in this publication.

DATES: This new system of records will become effective upon publication, subject to a 30-day comment period in which to comment on routine uses. To be considered, written comments must be submitted on or before July 18, 2022.

ADDRESSES: Please address comments to the Office of Inspector General Office of Counsel, Room 7896, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; by email to *OIGCounsel@oig.doc.gov;* or by facsimile to (202) 501–7335.

FOR FURTHER INFORMATION CONTACT: E. Wade Green, Jr., OIG Office of Counsel, email: *OIGCounsel@oig.doc.gov;* or Phone: (202) 792–3317.

SUPPLEMENTARY INFORMATION: The Department is creating a new system of records for OIG Data Analytics, entitled ''COMMERCE/OIG–2, OIG Data Analytics Records,'' as part of its commitment to ensuring that collection, use, retention, or dissemination of information about individuals through the use of any technology, including digitized archival records, complies with the law.

The Privacy Act requires each agency that proposes to establish a new system of records to provide adequate advance notice of any such proposal to the OMB, the Committee on Oversight and Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate (5 U.S.C 552a(r)). The purpose of providing the advance notice to OMB and Congress is to permit an evaluation of the potential effect of the proposal on the privacy and other rights of individuals. The Department filed a report describing the new system of records covered by this notice with the Chair of the Senate Committee on Homeland Security and Governmental Affairs, the Chair of the House Committee on Oversight and Reform, and the Deputy Administrator of the Office of Information and Regulatory Affairs, OMB, on March 30, 2022.

SYSTEM NAME AND NUMBER:

COMMERCE/OIG–2, OIG Data Analytics Records.

SECURITY CLASSIFICATION:

Controlled Unclassified Information (CUI).

SYSTEM LOCATION:

U.S. Department of Commerce, Office of Inspector General, 1401 Constitution Avenue NW, Washington, DC 20230.

SYSTEM MANAGER(S):

Chief of Staff to the Inspector General, Room 7709, Office of Inspector General, United States Department of Commerce, 1401 Constitution Ave. NW, Washington, DC 20230.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Inspector General Act of 1978, as amended, 5 U.S.C. App. (Inspector General Act).

PURPOSE(S) OF THE SYSTEM:

The records contained in this system are used or are available for use by the Office of Inspector General (OIG) to carry out its statutory responsibilities under the Inspector General Act to conduct and supervise audits, evaluations, inspections, and investigations, to prevent and detect fraud, waste, mismanagement, and abuse, and to promote economy, efficiency, and effectiveness in the Department of Commerce (the Department) programs and operations. The records may be used in the course of performing audits, evaluations, and inspections; investigating individuals and entities suspected of criminal, civil, or administrative misconduct and in supporting related judicial and administrative proceedings; or in conducting preliminary inquiries undertaken to determine whether to commence an audit, evaluation, inspection, or investigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

OIG maintains records in its records system on the following categories of individuals: current, former, and prospective Department employees; contractors; subcontractors; recipients of Federal funds and their contractors/subcontractors and employees; grantees; sub-grantees; individuals who work on Department grants (*e.g.,* principal investigators); lessees; licensees; persons engaged in official business with the Department; or other persons identified by OIG or by other agencies, constituent units of the Department, and members of the general public in connection with the authorized functions of the OIG.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains materials received, gathered, or created regarding or supporting Department operations. Categories of records may include: Commerce Business Systems information, including general ledger data, trial data, customer data, and vendor data; Department payroll, fleet card, purchase card, and travel card data; System for Award Management data; general case management documentation; correspondence; personally identifiable and business identifiable information, including financial, employment, time and attendance, human resources, and biometric data and Social Security Numbers; information protected by Title 13 of the U.S. Code; trade secrets data and similar proprietary data; import/export data, including Automated Export System data; law enforcement data; data containing information related to Department grants and contracts, and other data and evidence received, collected, or generated by OIG's Data Analytics group while conducting its official duties. Social Security Numbers are maintained in the system pursuant to authority under the Inspector General Act and are collected or received and maintained in the system as necessary by OIG to carry out its statutory responsibilities under the Inspector General Act.

RECORD SOURCE CATEGORIES:

As described below in ''Exemptions Promulgated for the System,'' the OIG claims an exemption from disclosure of record source categories under 5 U.S.C. 552a(e)(4)(I). Notwithstanding the foregoing, OIG may collect information from a wide variety of sources, including information from the Department and other Federal, State, and local agencies, and non-governmental entities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND 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 may be disclosed to authorized individuals and/or entities, as is determined to be compatible with the purposes for which the record was collected, as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. In the event that a record, either by itself or in combination with other information, indicates a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute or contract, or rule, regulation, or order issued pursuant thereto, or the necessity to protect an interest of the Department or OIG, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency or entity, whether federal, state, local, tribal, territorial, foreign, or international, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, or rule, regulation or order issued pursuant thereto, or protecting the interest of the Department or OIG.

2. To any source from which additional information is requested in order to obtain information relevant to: A decision by either the Department or OIG concerning the hiring, assignment, or retention of an individual or other personnel action; the issuance, renewal, retention, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance, retention, or revocation of a license, grant, award, contract, or other benefit to the extent the information is relevant and necessary to a decision by the Department or OIG on the matter.

3. To a Federal, State, local, tribal, territorial, foreign, international, or other public authority in response to its request in connection with: The hiring, assignment, or retention of an individual; the issuance, renewal, retention, or revocation of a security clearance; the reporting of an investigation of an individual; the execution of a security or suitability investigation; the letting of a contract; or the issuance, retention, or revocation of a license, grant, award, contract, or other benefit conferred by that entity to the extent that the information is relevant and necessary to the requesting entity's decision on the matter.

4. In the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to duly-authorized investigators or opposing parties in the course of discovery or settlement negotiations.

5. To a Member of Congress submitting a request involving an individual when the individual has requested assistance from the Member with respect to the subject matter of the record relating to the individual.

6. To the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular No. A–19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

7. To the Department of Justice (DOJ) or any other Federal agency that has an interest in the record in connection with determining whether disclosure thereof is required by the Freedom of Information Act (FOIA) (5 U.S.C. 552).

8. To contractors, grantees, consultants, or volunteers performing or working on a contract, service, grant, cooperative agreement, job, or other activity for the Department or OIG, who have a need to access the information in the performance of their duties or activities. When appropriate, recipients will be required to comply with the requirements of the Privacy Act as provided in 5 U.S.C. 552a(m).

9. To the Office of Personnel Management (OPM) for personnel research purposes; as a data source for management information; for the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained; or for related manpower studies.

10. To the General Services Administration (GSA) or the National Archives and Records Administration (NARA) during an inspection of records conducted by GSA or NARA under the authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA or NARA regulations governing inspection of records for this purpose and any other relevant (*i.e.,* GSA, NARA, or Department) directive. Such disclosure shall not be used to make determinations about individuals.

11. To appropriate agencies, entities, and persons when (1) the Department or the OIG suspects or has confirmed that there has been a breach of the system of records; (2) the Department or the OIG 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 or OIG's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

12. To another Federal agency or Federal entity, when the OIG 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.

13. To the Department of Justice (DOJ) and any other Federal agency, to the extent necessary to obtain their advice relevant to an OIG matter, including matters concerning the FOIA and the Privacy Act (5 U.S.C. 552a).

14. To the Office of Government Information Services (OGIS), NARA to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h) to review administrative policies, procedures, and compliance with the FOIA, and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

15. To the appropriate agency or entity, whether Federal, State, local, tribal, territorial, foreign, or international, charged with the responsibility for investigating or prosecuting a violation of any law, rule, regulation, or order. Routine use for law enforcement purposes also includes disclosure to individuals or to agencies, whether Federal, State, local, tribal, territorial, foreign, or international, when necessary to further the ends of an investigation.

16. To the DOJ or any other Federal agency that is responsible for representing Department interests in connection with judicial,

administrative, or other proceedings. This includes circumstances in which:

(1) the Department or OIG, or any component thereof;

(2) any employee of the Department or OIG in his or her official capacity;

(3) any employee of the Department or OIG in his or her individual capacity, where DOJ or other agency that is responsible for representing Department interests has agreed to represent or is considering a request to represent the employee; or

(4) the United States, or any of its components,

is a party to pending or potential judicial, administrative, or other proceeding or has an interest in such proceeding; the Department or OIG is likely to be affected by the proceeding; or the Department or OIG determines that the use of such records by the DOJ or any other Federal agency that is responsible for representing Department interests is relevant and necessary to the proceeding.

17. To any source from which additional information is requested, either private or governmental, to the extent necessary to solicit information relevant to any investigation, audit, evaluation, or inspection.

18. To a foreign government or international organization pursuant to an international treaty, convention, implementing legislation, or executive agreement entered into by the United States.

19. To representatives of OPM, the Office of Special Counsel, the Merit Systems Protection Board, the Federal Labor Relations Authority, the Equal Employment Opportunity Commission, the Office of Government Ethics, and other Federal agencies in connection with their efforts to carry out their responsibilities to conduct examinations, investigations, and/or settlement efforts, in connection with administrative grievances, complaints, claims, or appeals filed by an employee, or as may be authorized by law.

20. To a grand jury agent pursuant to a Federal or State grand jury subpoena or to a prosecution request that such record be released for the purpose of its introduction to a grand jury.

21. To the Departments of the Treasury and Justice in circumstances in which OIG seeks to obtain, or has in fact obtained, an ex parte court order to obtain tax return information from the Internal Revenue Service.

22. To any Federal official charged with the responsibility to conduct qualitative assessment reviews of internal safeguards and management procedures for purposes of reporting to the President and Congress on the activities of OIG. This disclosure category includes other Federal Offices of Inspectors General and members of the Council of the Inspectors General on Integrity and Efficiency, and officials and administrative staff within their chain of command, as well as authorized officials of DOJ and its component, the Federal Bureau of Investigation.

23. To the public or to the media for release to the public when (1) the matter under review has become public knowledge or the Inspector General determines that such disclosure is necessary to preserve confidence in the integrity of the OIG audit, evaluation, inspection, review, or investigative process, or is necessary to demonstrate the accountability of Department employees, officers, or individuals covered by the system; and (2) the Inspector General, after receipt of a written recommendation from Counsel to the Inspector General, makes a written determination that the release of the specific information in the context of a particular case would not constitute an unwarranted invasion of personal privacy.

24. To Congress, congressional committees, or the staffs thereof, in order to fulfill the Inspector General's responsibility, as mandated by the Inspector General Act, to keep the Congress fully and currently informed concerning fraud and other serious problems, abuses, and deficiencies concerning the administration of programs and operations administered or financed by the Department.

25. To a Federal, State, local, or foreign agency, or other public authority, for use in computer matching programs or similar activities, as authorized by the Inspector General Act, to prevent and detect fraud, waste, and abuse and to support civil and criminal law enforcement activities of any agency or its components.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Any electronic media (photographs, audio recording, diskettes, CDs, etc.) are kept in limited-access areas during duty hours and in locked offices during nonduty hours. Electronic records are maintained on servers, which house OIG's electronic systems. Servers are maintained in a secured, restricted-area facility.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Electronic searches may be performed by search criteria that include names of individuals, names of businesses, identifying particulars, organizations, and other key word search variations.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with OIG Records Retention Schedules approved by NARA.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Any electronic media are kept in limited-access areas during duty hours and in locked offices during nonduty hours and are used only by authorized screened personnel. Electronic records are stored on servers maintained in a locked facility that is secured at all times by security systems and video cameras. Data in the system are encrypted and password protected. Access to electronic records is restricted to OIG staff and contractors individually authorized to access the electronic system. Passwords are changed periodically, in accordance with OIG policy. Backup tapes are stored in a locked and controlled room in a secure off-site facility.

RECORD ACCESS PROCEDURES:

The Inspector General has exempted this system from the access procedures of the Privacy Act.

CONTESTING RECORD PROCEDURES:

The Inspector General has exempted this system from contesting record procedures of the Privacy Act.

NOTIFICATION PROCEDURES:

The Inspector General has exempted this system from the procedures of the Privacy Act relating to individuals' requests for notification of the existence of records on themselves.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Under 5 U.S.C. 552a(j)(2), the head of any agency may exempt any system of records within the agency from certain provisions of the Privacy Act, if the agency or component that maintains the system performs as its principal function any activities pertaining to the enforcement of criminal laws. The Inspector General Act mandates that the Inspector General recommend policies for, and conduct, supervise, and coordinate activities in the Department and between the Department and other Federal, State, and local government agencies with respect to all matters relating to the prevention and detection of fraud in programs and operations administered or financed by the Department, and to the identification and prosecution of participants in such fraud. Under the Inspector General Act,