Billing Code

DEPARTMENT OF COMMERCE

[Docket No. 210923-0194]

Privacy Act of 1974; System of Records

AGENCY: Department of Commerce, Office of the Secretary.

ACTION: Notice of a new system of records.

SUMMARY: This notice announces the Department of Commerce's (Department) proposal to establish a new system of records entitled "COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations" under the Privacy Act of 1974, 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 describes the Department's collection, use, and maintenance of records on individuals associated with the Department and its facilities during a public health emergency or similar health and safety incident. This newly established system will be included in the Department's inventory of record systems. 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 the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may submit written comments to Tahira Murphy, Acting Program Director for Privacy Act Compliance, tmurphy2@doc.gov.

FOR FURTHER INFORMATION CONTACT: Tahira Murphy, Acting Program Director for Privacy Act Compliance, (202) 482-8075.

SUPPLEMENTARY INFORMATION: The Department of Commerce must ensure the safety of its workforce and the public, including when the Secretary of Health and Human Services

(HHS) or other designated official determines and declares that a public health emergency exists or when a similar health and safety emergency or incident occurs. Responses to public health emergencies or similar health and safety incidents depend on the nature of the emergency or incident, but in the context of an infectious disease outbreak, or a pandemic or epidemic that can cause widespread harm to the health of individuals, the Department of Commerce may collect information on Department personnel (including employees, detailees, guest researchers, affiliates, interns, and volunteers), contractors, long-term trainees, mission support individuals, and visitors at or on Department locations (including buildings, grounds, ships, aircraft, vehicles, or properties that are owned or leased by the Department; otherwise used by the Department for meetings, conferences, events, or other official business; or contractor or subcontractor workplace locations and individuals in those locations working on or in connection with a Federal Government contract or contract-like instrument) in order to ensure a safe and secure work environment. The information collected may include names and contact information; individual circumstances and dates of suspected exposure; testing results, symptoms, and treatments; health status information, and other information related to the public health emergency. For federal employees, in certain instances, depending on the type of record collected and maintained, this information will also be maintained and covered by OPM/GOVT-10, Employee Medical File System Records, 75 FR 35099 (June 21, 2010), and modified at 80 FR 74815 (Nov. 30, 2015). However, any collection and use of records covered by COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations, is only permitted during times of a public health emergency or similar health and safety incident and when the circumstances permit the Department to collect and maintain such information on the various categories of Department personnel, contractors, long-term trainees, mission support individuals, and visitors at Department locations.

The circumstances must be examined in conjunction with all applicable laws, including the U.S. Constitution, federal privacy laws, federal labor and employment laws, and federal workforce health and safety laws. Different laws may apply depending upon the type of information at issue, who the information pertains to, who collected the information, and how the information is collected, maintained, and used by the Department.

For instance, when collecting information on Department employees, there are several employment laws that govern the collection, dissemination, and retention of employee medical information. These employment laws include the Americans with Disabilities Act of 1990, as amended (ADA), the Rehabilitation Act of 1973 (Rehab Act), and the Occupational Safety and Health Act of 1970 (OSH Act). Generally, under federal employment laws, medical information pertaining to employees is confidential and may be obtained by an employer only for certain reasons and only at certain points in the employment relationship. During a public health emergency, an employer may be permitted to collect certain employee medical information that it would not otherwise be permitted to collect depending upon the circumstances. Whether an employer is permitted to collect otherwise confidential employee medical information during a public health emergency depends upon whether an employee or a potential employee poses a "direct threat" to others within the meaning of the ADA and the Rehab Act. Again, this system of records will apply if it is determined that the circumstances permit the Department to legally collect the employee medical information at issue in the first instance.

Information stored in this system of records may be shared with other Department components that have a need to know the information to carry out their mission essential functions, but only if it is first determined that the information may be shared under all other applicable laws and Department policies.

In addition, the Department may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth

in this system of records notice, but, again, only if it is first determined that the information may be shared under all other applicable laws and Department policies.

This newly established system will be included in the Department's inventory of record systems.

Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations, system of records.

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

SYSTEM NAME AND NUMBER: COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations.

SECURITY CLASSIFICATION: Controlled Unclassified Information.

SYSTEM LOCATION: Records are maintained at the Department of Commerce (Department) Headquarters, component offices, field offices, and contractor-owned and operated facilities.

SYSTEM MANAGER AND ADDRESS: Director, Office of Privacy and Open Government, U.S. Department of Commerce, 1401 Constitution Ave, NW, Room 61025, Washington, D.C. 20230.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Section 319 of the Public Health Service (PHS) Act (42 U.S.C. 247d); Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law 116-136, Div. B., Title VIII, sec. 18115, 134 Stat. 574 (codified in 42 U.S.C. 247d note); 21 U.S.C. 360bbb-3; Rehabilitation Act, 29 U.S.C. 701 et. seq.; Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d); 29 CFR part 1602; 29 CFR part 1630; Medical Examinations for Fitness for Duty Requirements, including 5 CFR part 339; Workforce safety federal requirements, including the Occupational Safety and Health Act of 1970, Executive Order 12196, 5 U.S.C. 7902; 29 U.S.C. chapter 15 (e.g., 29 U.S.C. 668), 29 CFR part 1904, 29 CFR part 1910, and 29 CFR part 1960; and the Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. 2000ff to ff-11, and 29 CFR part 1635; and other federal laws, regulations, Executive orders, or guidance related to the specific public health emergency or similar health and safety incident, including guidance issued by the Office of Management and Budget, the Centers for Disease Control and Prevention, or other appropriate agency or entity, as applicable.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to maintain records to protect the Department's workforce and other individuals at or on “Department locations”—which is defined to include buildings, grounds, ships, aircraft, vehicles, or properties that are owned or leased by the Department; otherwise used by the Department for meetings, conferences, events, or other official business; or contractor or subcontractor workplace locations and individuals in those locations working on or in connection with a Federal Government contract or contract-like instrument—and respond to or mitigate a public health emergency or similar health and safety incident. For instance, the Department may use the information collected to conduct contact tracing (i.e., the subsequent identification, monitoring, and support of a confirmed or probable

case's close contacts who have been exposed to, and possibly infected with, a disease or illness at or on Department locations); institute preventative testing or other measures to permit entry to Department locations to minimize exposure; and fulfill testing reporting requirements, to the extent permitted by law.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Department personnel (including employees, detailees, guest researchers, affiliates, interns, and volunteers), long-term trainees (such as Honors graduates, Pathways employees, Temporary, Not-to-Exceed (NTE) employees, Knauss Fellows, etc.), contractors, mission support individuals, visitors (such as all other federal employees, applicants, and members of the public) at or on Department locations, and potentially affected individuals otherwise present during official Department business. For example, individuals covered by this system may include those who are suspected or confirmed to have a disease or illness that is the subject of a public health emergency, may have been or could have been exposed to someone who is suspected or confirmed to have a disease or illness that is the subject of a public health emergency, or who must undergo preventative testing or treatment (e.g., vaccines) for a disease or illness that is the subject of a public health emergency. Mission support individuals include those individuals who are assigned from other federal, state, local, or private agencies to support Department missions and operations at Department locations. The system also covers individuals listed as emergency contacts for such individuals.

CATEGORIES OF RECORDS IN THE SYSTEM: The records in this system include information related to the public health emergency or similar health and safety incident that is relevant and necessary to achieve the purpose of this system or records, which may vary depending on the nature of the specific emergency or incident. For Department personnel, long-term trainees, contractors, and mission support individuals, the information collected may include, for example: Individual's full name; Preferred phone number(s); Department duty location, facility, and specific work space accessed; Preferred email address(es); Individual's supervisor’s name, address, and contact information, and/or the contractor's

supervisor/contracting officer representative name, address, and contact information; Date(s) and circumstances of the individual's suspected or actual exposure to disease or illness including symptoms, as well as locations within the Department workplace where an individual may have contracted or been exposed to the disease or illness, and names and contact information of other employees, long-term trainees, contractors, mission support individuals, or visitors that the individual interacted with at or on a Department location during time the individual was suspected to or had contracted the disease or illness; Work status of the individual (e.g., administrative leave, sick leave, teleworking, in the office, deployed to the field) and affiliated leave status information; Emergency contact information; Other individual information directly related to the disease or illness, such as vaccination status, testing results/information, symptoms, source of potential exposure, or prior infection status; Other information for identification verification purposes when disclosing testing results or other health emergency data to third-parties; and Information collected in accordance with CARES Act reporting requirements or other statutory, regulatory, and administrative reporting requirements. For visitors at Department locations, the information collected may include, for example: Full name; Preferred phone number(s); Preferred email address(es); Date(s) and time(s) of entrance and exit from Department workspaces, ships, aircraft, facilities, and grounds; Name(s) of all individuals encountered while in or at Department locations; Public-health emergency-related data, such as vaccination status, testing results/information, symptoms, source of potential exposure, or prior infection status; Emergency contact information; and Information indicating plans on entering a Department location in the near future.

RECORD SOURCE CATEGORIES: When permitted by applicable law, records may be obtained from Department personnel, long-term trainees, contractors, mission support individuals, and visitors at or on Department locations; their family members; federal, state, local, tribal, territorial, and foreign government agencies; employers; and other entities and individuals who may provide relevant information on a suspected or confirmed disease or illness

that is the subject of a public health emergency. Records in this system may also be obtained from security systems or other systems of records, such as OPM/GOVT-10.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In the event the Department's Senior Agency Official for Privacy or other senior Department privacy official determines, in consultation with the Office of the General Counsel, that disclosure of a record contained in this system is not prohibited by the Rehabilitation Act or other applicable laws, regulations, or policies, that record may be disclosed as generally permitted by the Privacy Act and for the following routine uses pursuant to 5 U.S.C. 552a(b)(3):

1. In the event that a system of records maintained by the Department to carry out its functions 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, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local or foreign, 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.

2. A record from this system of records may be disclosed, as a routine use, to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

3. A record from this system of records may be disclosed, as a routine use, to a federal, state, local, or international agency, in response to its request, in connection with the issuance of a security clearance, the reporting of an investigation of an individual, the letting of a contract, or

the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate or administrative tribunal, including disclosures to duly-authorized investigators or opposing counsel in the course of discovery or settlement negotiations.

5. A record in this system of records may be disclosed, as routine use, 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.

6. A record in this system of records which contains medical information may be disclosed, as a routine use, to the medical advisor of any individual submitting a request for access to the record under the Act and 15 CFR part 4, subpart B if, in the sole judgment of the Department, disclosure directly to the individual could have an adverse effect upon the individual, under the provision of 5 U.S.C. 552a(f)(3) and implementing regulations at 15 CFR 4.26.

7. (Reserved)

8. A record in this system of records may be disclosed, as a routine use, to the Office of Management and Budget 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.

9. A record in this system of records may be disclosed, as a routine use, to the Department of Justice in connection with determining whether disclosure thereof is required by the Freedom of Information Act (5 U.S.C. 552).

10. A record in this system of records may be disclosed, as a routine use, to a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m).

11. (Reserved)

12. A record in this system may be transferred, as a routine use, to the Office of Personnel Management: 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.

13. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services Administration (GSA), or his designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Department of Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

14. A record in this system of records may be disclosed 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.

15. A record in this system of records may be disclosed 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. A record in this system of records may be disclosed to student volunteers, individuals working under a personal services contract, and other workers who technically do not have the status of Federal employees, when they are performing work for the Department and/or its operating units, as authorized by law, as needed to perform their assigned functions.

17. A record in this system may be disclosed to the Department of Treasury for the purpose of reporting and recouping delinquent debts owed the United States pursuant to the Debt Collection Improvement Act of 1996.

18. A record in this system may be disclosed to an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

19. A record in this system of records may be disclosed to appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease, to combat other significant public health threats, or to identify mission critical personnel appropriate for potential early vaccination or other treatment options.

20. A record in this system of records may be disclosed to such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

21. A record in this system of records may be disclosed to Federal agencies such as the Department of Health and Human Services (HHS), State and local health departments, and other public health or cooperating medical authorities in connection with program activities and related collaborative efforts to deal more effectively with exposures to communicable diseases, and to satisfy mandatory reporting requirements when applicable.

22. A record in this system of records may be disclosed to a potentially affected individual's emergency contact for purposes of locating the individual to communicate that they may have been exposed to a public health emergency contaminant in a Department location, while

otherwise present during official Department business, or at contractor or subcontractor workplace locations where individuals in those locations were working on or in connection with a Federal Government contract or contract-like instrument.

23. A record in this system of records may be disclosed to affected individuals or potentially affected individuals, or, when needed, to the (potentially) affected individual's employer, grantee organization, federal agency to whom the individual is contracted, or other similar designated external points of contact, to the extent the information is necessary for contact tracing.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system of records are stored electronically or on paper in secure facilities. Electronic records are stored on a secure network. Records are protected from unauthorized access and improper use through administrative, technical, and physical security measures. Medical information collected is maintained on separate forms and in separate medical files and is treated as a confidential medical record.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The Department may retrieve records by any of the categories of records, including name, location, date of vaccination, date of potential exposure, or work status.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: All records are retained and disposed of in accordance with National Archive and Records Administration regulations (36 CFR chapter XII, subchapter B – Records Management); Departmental directives and comprehensive records schedules; and, to the extent applicable, NOAA Administrative Order 205-01 or other directives issued by a Departmental component. To the extent applicable, to ensure compliance with the Americans with Disabilities Act (ADA), the Rehabilitation Act, and the Genetic Information Nondiscrimination Act of 2008 (GINA), medical information must be maintained on separate forms and in separate medical files and be treated as a confidential medical record. 42 U.S.C. 12112(d)(3)(B); 42 U.S.C. 2000ff-5(a); 29 CFR 1630.14(b)(1), (c)(1), (d)(4)(i); and 29 CFR 1635.9(a). This means that medical

information and documents must be stored separately from other personnel records. As such, the Department must keep medical records for at least one year from creation date. 29 CFR 1602.14. Further, any records compiled under this system and incorporated into an occupational individual medical case record pursuant to the OSH Act must be maintained in accordance with 5 CFR 293.511(b) and 29 CFR 1910.1020(d), and must be destroyed 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer, in accordance with NARA General Records Schedule (GRS) 2.7, Item 60, and NARA records retention schedule DAA-GRS-2017-0010-0009, to the extent applicable. Visitor processing records are covered by GRS 5.6, Items 110 and 111, and must be destroyed when either two or five years old, depending on security level, but may be retained longer if required for business use, pursuant to DAA-GRS-2017-0006-0014 and -0015.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The system of records is stored in buildings with doors that are locked during and after business hours. Visitors to the facility must register with security guards and must be accompanied by Federal personnel at all times. Records are stored in a locked room and/or a locked file cabinet. Electronic records containing Privacy Act information are protected by a user identification/password. The user identification/password is issued to those individuals who have a need to access the records for the performance of their official duties and who have appropriate clearances or permissions. Technical security safeguards include restrictions on computer access to authorized individuals who have a legitimate need to know the information; required use of strong passwords that are frequently changed; multi-factor authentication for remote access; use of encryption for certain data types and transfers; firewalls and intrusion detection applications; and regular review of security procedures and best practices to enhance security. Physical safeguards include restrictions on building access to authorized individuals and storage of records in locked offices and filing cabinets.

All electronic information disseminated by the Department adheres to the standards set out in Appendix III, Security of Automated Information Resources, OMB Circular A-130; the Computer Security Act (15 U.S.C. 278g-3 and 278g-4); and the Government Information Security Reform Act, Public Law 106-398; and follows NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems; NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems; and NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

RECORD ACCESS PROCEDURES: Requests from individuals should be addressed to: Chief Privacy Officer, U.S. Department of Commerce, Office of Privacy and Open Government, 1401 Constitution Ave, NW, Room 61025, Washington, D.C. 20230, pursuant to 15 CFR part 4, Subpart B.

CONTESTING RECORD PROCEDURES: The Department's rules for access, contesting contents, and appealing initial determinations by the individual concerned appear in 15 CFR part 4, Subpart B. Use address cited in Record Access Procedures above.

NOTIFICATION PROCEDURES: Requests for notification of the existence of records pertaining to the requester should be submitted pursuant to the inquiry provisions of the Department's rules which appear in 15 CFR part 4, subpart B. Use address cited in Record Access Procedures above.

EXEMPTIONS CLAIMED FOR THE SYSTEM: None.

HISTORY: No history.

Notice of New System of Record.

Jennifer Goode,

Department of Commerce,

Acting Chief Privacy Officer and Director,

Office of Privacy and Open Government.

[FR Doc. 2021-25136 Filed: 11/17/2021 8:45 am; Publication Date: 11/18/2021]