7600-01-M

OCCUPATIONAL SAFETY AND HEALTH REVIEW COMMISSION

Privacy Act of 1974; System of Records

AGENCY: Occupational Safety and Health Review Commission.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the Occupational Safety and Health Review Commission (OSHRC) is revising the notice for Privacy Act system-of-records OSHRC-6.

DATES: Comments must be received by OSHRC on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The revised system of records will become effective on that date, without any further notice in the *Federal Register*, unless comments or government approval procedures necessitate otherwise.

ADDRESSES: You may submit comments by any of the following methods:

- E-mail: rbailey@oshrc.gov. Include "PRIVACY ACT SYSTEM OF RECORDS" in the subject line of the message.
- Fax: (202) 606-5417.
- Mail: One Lafayette Centre, 1120 20th Street NW, Ninth Floor, Washington, DC 20036-3457.
- Hand Delivery/Courier: same as mailing address.

Instructions: All submissions must include your name, return address, and e-mail address, if applicable. Please clearly label submissions as "PRIVACY ACT SYSTEM OF RECORDS."

FOR FURTHER INFORMATION CONTACT: Ron Bailey, Attorney-Advisor, Office of the General Counsel, via telephone at (202) 606-5410, or via e-mail at rbailey@oshrc.gov.

SUPPLEMENTARY INFORMATION: The Privacy Act of 1974, 5 U.S.C. 552a(e)(4), requires federal agencies such as OSHRC to publish in the *Federal Register* notice of any new or modified system of records.

As detailed below, OSHRC is revising the name of the company that operates the government-only cloud in which electronic records are maintained, the physical location of the facility that maintains the cloud, and safeguards used at that facility.

In addition, OSHRC recently revised its Privacy Act regulations, 29 C.F.R. pt. 2400, which resulted in the renumbering of its regulatory provisions. 85 FR 65222 (Oct. 15, 2020). OSHRC is therefore revising the following elements in this system-of-records notice to reference the correct sections of the agency's Privacy Act regulations: Record Access Procedures, Contesting Record Procedures, and Notification Procedures.

The notice for OSHRC-6, provided below in its entirety, is as follows.

SYSTEM NAME AND NUMBER: E-Filing/Case Management System, OSHRC-6.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Electronic records are maintained in a government-only cloud within an Oracle Database, operated by Tyler Federal, LLC, at 44470 Chilum Place, Ashburn, VA 20148. Paper records are maintained by the Office of the Executive Secretary, located at 1120 20th Street, NW, Ninth Floor, Washington, DC 20036–3457.

SYSTEM MANAGER(S): Supervisory Information Technology Specialist (electronic records contained in the e-filing/case management system) and the Executive Secretary (all other records), OSHRC, 1120 20th Street, NW, Ninth Floor, Washington, DC 20036–3457; (202) 606-5100.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 29 U.S.C. 661.

PURPOSE(S) OF THE SYSTEM: This system of records is maintained for the purpose of processing cases that are before OSHRC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system of records covers (1) ALJs; (2) Commission members and their staff; (3) OSHRC employees entering data into the e-filing/case management system, or assigned responsibilities with respect to a particular case; and (4) parties, the parties' points of contact, and the parties' representatives in cases that have been, or presently are, before OSHRC.

CATEGORIES OF RECORDS IN THE SYSTEM: The electronic records contain the following information: (1) The names of those covered by the system of records and, as to parties, their points of contact; (2) the telephone and fax numbers, business email addresses, and/or business street addresses of those covered by the system of records; (3) the names of OSHRC cases, and information associated with the cases, such as the inspection number, the docket number, the state in which the action arose, the names of the representatives, and whether the case involved a fatality; (4) events occurring in cases and the dates on which the events occurred; (5) documents filed in cases and the dates on which the documents were filed; and (6) the names of OSHRC employees entering data into the e-filing/case management system, or assigned responsibilities with respect to a particular case. The paper records are hard copies of the electronic records in the e-filing/case management system.

RECORD SOURCE CATEGORIES: Information in this system is derived from the individual to whom it applies or is derived from case processing records maintained by the Office of the Executive Secretary and the Office of the General Counsel, or from information provided by the parties who appear before OSHRC.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to 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 the Department of Justice (DOJ), or to a court or adjudicative body before which OSHRC is authorized to appear, when any of the following entities or individuals—(a) OSHRC, or any of its components; (b) any employee of OSHRC in his or her official capacity; (c) any employee of OSHRC in his or her individual capacity where DOJ (or OSHRC where it is authorized to do so) has agreed to represent the employee; or (d) the United States, where OSHRC determines that litigation is likely to affect OSHRC or any of its components—is a party to litigation or has an interest in such litigation, and OSHRC determines that the use of such records by DOJ, or by a court or other tribunal, or another party before such tribunal, is relevant and necessary to the litigation.

(2) To an appropriate agency, whether federal, state, local, or foreign, charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes civil, criminal or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

(3) To a federal, state, or local agency maintaining civil, criminal or other relevant enforcement information, such as current licenses, if necessary, to obtain information relevant to an OSHRC decision concerning the hiring, appointment, or retention 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 license, grant or other benefit.

(4) To a federal, state, or local agency, in response to that agency's request for a

record, and only to the extent that the information is relevant and necessary to the requesting agency's decision in the matter, if the record is sought in connection with the hiring, appointment, or retention 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 license, grant or other benefit by the requesting agency.

(5) To an authorized appeal grievance examiner, formal complaints manager, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee, only to the extent that the information is relevant and necessary to the case or matter.

(6) To OPM in accordance with the agency's responsibilities for evaluation and oversight of federal personnel management.

(7) To officers and employees of a federal agency for the purpose of conducting an audit, but only to the extent that the record is relevant and necessary to this purpose.

(8) To OMB in connection with the review of private relief legislation at any stage of the legislative coordination and clearance process, as set forth in Circular No. A-19.

(9) To a Member of Congress or to a person on his or her staff acting on the Member's behalf when a written request is made on behalf and at the behest of the individual who is the subject of the record.

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

(11) To appropriate agencies, entities, and persons when: (a) OSHRC suspects or has confirmed that there has been a breach of the system of records; (b) OSHRC has

determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, OSHRC, the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with OSHRC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

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

(13) To another federal agency or federal entity, when OSHRC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) 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.

(14) To a bar association or similar federal, state, or local licensing authority for a possible disciplinary action.

(15) To vetted employees of Tyler Federal, LLC, in order to ensure that the e-filing/case management system is properly maintained.

(16) To the public, in accordance with 29 U.S.C. 661(g), for the purpose of inspecting and/or copying the records at OSHRC.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: At the Equinix secure colocation site, the information is stored in a database contained on a separate database server behind the application server serving the data. Paper records are stored in the records room and in file cabinets.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Electronic records contained in the case e-filing/case management system may be retrieved by any of the data items listed under "Categories of Records in the System," including docket number, inspection number, any part of a representative's name or the case name, and user. Paper records may be retrieved manually by docket number or case name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Under Records Disposition Schedule N1-455-90-1, paper case files may be destroyed 20 years after a case closes. Under Records Disposition Schedule N1-455-11-2, electronic records pertaining to those paper case files may be deleted when no longer needed for the conduct of current business.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Electronic records contained in the e-filing/case management system are safeguarded as follows. Data going across the Internet is encrypted using SSL encryption. Every system is password protected. Tyler Federal, LLC, which stores the data in a government-only cloud within an Oracle Database, operates its own equipment that is protected by physical security measures. Only authorized employees of Tyler Federal, LLC, who have both biometric and PIN access to the datacenter cage utilized by Tyler Federal, LLC, can physically access the sites where data is stored. Only authorized and vetted employees of Tyler Federal, LLC, have access to the servers containing any PII.

The access of parties and their representatives to electronic records in the system is limited to active files pertaining to cases in which the parties are named, or the representatives have entered appearances. The access of OSHRC employees is limited to personnel having a need for access to perform their official functions and is additionally restricted through password identification procedures.

Paper records are maintained in a records room that can only be accessed using a smartcard or a key. Some paper records are also maintained in file cabinets. During duty

hours, these records are under surveillance of personnel charged with their custody, and after duty hours, the records are secured behind locked doors. Access to the cabinets is limited to personnel having a need for access to perform their official functions.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to their records should notify: Privacy Officer, OSHRC, 1120 20th Street, NW, Ninth Floor, Washington, DC 20036–3457. For an explanation on how such requests should be drafted, refer to 29 CFR 2400.4 (procedures for requesting notification of and access to personal records).

CONTESTING RECORD PROCEDURES: Individuals who wish to contest their records should notify: Privacy Officer, OSHRC, 1120 20th Street, NW, Ninth Floor, Washington, DC 20036–3457. For an explanation on the specific procedures for contesting the content of a record, refer to 29 CFR 2400.6 (procedures for amending personal records), and 29 CFR 2400.7 (procedures for appealing).

NOTIFICATION PROCEDURES: Individuals interested in inquiring about their records should notify: Privacy Officer, OSHRC, 1120 20th Street, NW, Ninth Floor, Washington, DC 20036–3457. For an explanation on how such requests should be drafted, refer to 29 CFR 2400.4 (procedures for requesting notification of and access to personal records).

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: July 7, 2016, 81 FR 44335; September 28, 2017, 82 FR 45324; and August 30, 2018, 83 FR 44309.

Nadine N. Mancini,

General Counsel,

Senior Agency Official for Privacy.

[FR Doc. 2021-19774 Filed: 9/13/2021 8:45 am; Publication Date: 9/14/2021]