Occupational Safety and Health Review Commission

Privacy Impact Assessment (PIA) for the
OSHRC E-Filing System (OSHRC - EFS) Information System

November 2016

OSHRC Office: Office of General Counsel, Privacy Office

Privacy Analyst: Ron Bailey
Telephone Number: 202-606-5410
E-mail Address: rbailey@oshrc.gov

The *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, requires Federal agencies to take special measures to protect personal information about individuals when the agencies collect, maintain, and use such personal information.

The Privacy Impact Assessment[1] template's purpose is to help the bureau/office to evaluate the changes in the information in the system and to make the appropriate determination(s) about how to treat this information, as required by the Privacy Act's regulations.

Section 1.0 Information System's Contents:

1.1 Status of the Information System[2]:

☒ New information system—Implementation date: 9/2016
☐ Revised or upgraded information system—Revision or upgrade date:

If this system is being revised—what will be done with the newly derived information:

☐ Placed in existing information system—Implementation Date:
☐ Placed in new auxiliary/ancillary information system—Date:
☐ Other use(s)—Implementation Date:

Please explain your response:

OSHRC has migrated from an in-house managed case tracking system to a FedRAMP certified cloud-based solution that allows litigants to file pleadings electronically.

1.2 Has a Privacy Threshold Assessment (PTA) been done?

☒ Yes
Date: 10/2016

☐ No

If a PTA has not been done, please explain why not:

If the Privacy Threshold Assessment (PTA) has been completed, please skip to Question 1.10

1.3 Has this information system, which contains information about individuals, *e.g.*, personally identifiable information (PII), existed under another name, *e.g.*, has the name been changed or modified?

☐ Yes
☐ No

Please explain your response:

1.4 Has this information system undergone a "substantive change" in the system's format or operating system?

☐ Yes
☐ No

[1] This questionnaire is used to analyze the impacts on the privacy and security of the personally identifiable information (PII) that is being maintained in these records and files.

[2] "Information system" is a general term that refers to electronic databases, licensing, and records systems and formats and also to paper based records and filing systems.

If yes, please explain your response:

If there have been no changes to the information system's format or operating system(s), please skip to Question 1.6.

1.5 Has the medium in which the information system stores the records or data in the system changed:

☐ Paper files to electronic medium (computer database);
☐ From one IT (electronic) information system to IT system, *i.e.*, from one database, operating system, or software program, *etc*.

Please explain your response:

1.6 What information is the system collecting, analyzing, managing, using, and/or storing, *etc.*:

Information about OSHRC Employees:

☐ No OSHRC employee information
☐ OSHRC employee's name
☐ Other names used, *i.e.*, maiden name, *etc*.
☐ OSHRC badge number (employee ID)
☐ SSN
☐ Race/Ethnicity
☐ Gender
☐ U.S. Citizenship
☐ Non-U.S. Citizenship
☐ Biometric data
  ☐ Fingerprints
  ☐ Voiceprints
  ☐ Retina scans/prints
  ☐ Photographs
  ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
☐ Birth date/age
☐ Place of birth
☐ Medical data
☐ Marital status
☐ Spousal information
☐ Miscellaneous family information
☐ Home address
☐ Home address history
☐ Home telephone number(s)
☐ Personal cell phone number(s):
☐ Personal fax number(s)
☐ E-mail address(es): OSHRC e-mail address.
☐ Emergency contact data:
☐ Credit card number(s)
☐ Driver's license
☐ Bank account(s)
☐ OSHRC personal employment records
☐ Military records
☐ Financial history
☐ Foreign countries visited

- ☐ Law enforcement data
- ☐ Background investigation history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☐ Other information:

Information about OSHRC Contractors:

- ☐ No OSHRC contractor information
- ☐ Contractor's name
- ☐ Other name(s) used, *i.e.*, maiden name, *etc*.
- ☐ OSHRC Contractor badge number (Contractor ID)
- ☐ SSN
- ☐ U.S. Citizenship
- ☐ Non-U.S. Citizenship
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Biometric data
  - ☐ Fingerprints
  - ☐ Voiceprints
  - ☐ Retina scans/prints
  - ☐ Photographs
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
- ☐ Birth date/Age
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information
- ☐ Home address
- ☐ Home address history
- ☐ Home telephone number(s)
- ☐ Personal cell phone number(s):
- ☐ Personal fax number(s)
- ☐ Personal e-mail address(es):
- ☐ Emergency contact data:
- ☐ Credit card number(s)
- ☐ Driver's license number(s)
- ☐ Bank account(s)
- ☐ Non-OSHRC personal employment records
- ☐ Military records
- ☐ Financial history
- ☐ Foreign countries visited
- ☐ Law enforcement data
- ☐ Background investigation history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☐ Other information:

Information about OSHRC Volunteers, Visitors, Customers, and other Individuals:

- ☐ Not applicable
- ☐ Individual's name:
- ☐ Other name(s) used, *i.e.*, maiden name, *etc*.
- ☐ OSHRC badge number (employee ID)
- ☐ SSN:
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Citizenship
- ☐ Non-U.S. Citizenship
- ☐ Biometric data
  - ☐ Fingerprints
  - ☐ Voiceprints
  - ☐ Retina scans/prints
  - ☐ Photographs
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
- ☐ Birth date/Age:
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information
- ☐ Home address
- ☐ Home address history
- ☐ Home telephone number(s)
- ☐ Personal cell phone number(s):
- ☐ Personal fax number(s)
- ☐ Personal e-mail address(es):
- ☐ Emergency contact data:
- ☐ Credit card number(s)
- ☐ Driver's license number(s)
- ☐ Bank account(s)
- ☐ Non-OSHRC personal employment records
- ☐ Military records
- ☐ Financial history
- ☐ Foreign countries visited
- ☐ Law enforcement data
- ☐ Background investigation history
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Digital signature
- ☐ Other information:

Information about Business Customers and others (usually not considered "personal information"):

- ☐ Not applicable
- ☐ Name of business contact/firm representative, customer, and/or others
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Full or partial SSN:
- ☐ Business/corporate purpose(s)
- ☐ Other business/employment/job description(s)

- ☐ Professional affiliations
- ☐ Business/office address
- ☐ Intra-business office address (office or workstation)
- ☐ Business telephone number(s)
- ☐ Business cell phone number(s)
- ☐ Business fax number(s)
- ☐ Business pager number(s)
- ☐ Business e-mail address(es)
- ☐ Bill payee name
- ☐ Bank routing number(s)
- ☐ Income/Assets
- ☐ Web navigation habits
- ☐ Commercially obtained credit history data
- ☐ Commercially obtained buying habits
- ☐ Credit card number(s)
- ☐ Bank account(s)
- ☐ Other information:

1.7 What are the sources for the PII and other information that this information system (or database) is collecting:

- ☐ Personal information from OSHRC employees:
- ☐ Personal information from OSHRC contractors:
- ☐ Personal information from non-OSHRC individuals and/or households:
- ☐ Non-personal information from businesses and other for-profit entities:
- ☐ Non-personal information from institutions and other non-profit entities:
- ☐ Non-personal information from farms:
- ☐ Non-personal information from Federal Government agencies:
- ☐ Non-personal information from state, local, or tribal governments:
- ☐ Other sources:

1.8 Does this information system have any links to other information systems or databases?

An information system (or database) may be considered as linked to other information systems (or databases) if it has one or more of the following characteristics:

- ☐ The information system is a subsystem or other component of another information system or database that is operated by another OSHRC bureau/office or non-OSHRC entity (like the FBI, DOJ, National Finance Center, etc.);
- ☐ The information system transfers or receives information, including PII, between itself and another OSHRC or non-OSHRC information system or database:
- ☐ The information system has other types of links or ties to other OSHRC or non-OSHRC information systems or databases;
- ☐ The information system has other characteristics that make it linked or connected to another OSHRC or non-OSHRC information system or database;
- ☐ The information system has no links to another information system (or database), *i.e.*, it does not share, transfer, and/or obtain data from another system.

Please explain your response:

1.9 What PII does the information system obtain, share, and/or use from other information systems?

- ☐ OSHRC information system and information system name(s):
- ☐ Non-OSHRC information system and information system name(s):

- ☐ OSHRC employee's name:
- ☐ (non-OSHRC employee) individual's name
- ☐ Other names used, *i.e.*, maiden name, *etc*.
- ☐ OSHRC badge number (employee ID)
- ☐ Other Federal Government employee ID information, *i.e.*, badge number, *etc*.
- ☐ SSN:
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ U.S. Citizenship
- ☐ Non-U.S. Citizenship
- ☐ Biometric data
  - ☐ Fingerprints
  - ☐ Voiceprints
  - ☐ Retina scan/prints
  - ☐ Photographs
  - ☐ Other physical information, *i.e.*, hair color, eye color, identifying marks, *etc*.
- ☐ Birth date/Age
- ☐ Place of birth
- ☐ Medical data
- ☐ Marital status
- ☐ Spousal information
- ☐ Miscellaneous family information:
- ☐ Home address
- ☐ Home address history
- ☐ Home telephone number(s)
- ☐ Personal cell phone number(s)
- ☐ Personal fax number(s)
- ☐ E-mail address(es): OSHRC e-mail address.
- ☐ Emergency contact data
- ☐ Credit card number(s)
- ☐ Driver's license
- ☐ Bank account(s)
- ☐ Non-OSHRC personal employment records
- ☐ Non-OSHRC government badge number (employee ID)
- ☐ Law enforcement data
- ☐ Military records
- ☐ National security data
- ☐ Communications protected by legal privileges
- ☐ Financial history
- ☐ Foreign countries visited
- ☐ Background investigation history
- ☐ Digital signature
- ☐ Other information:

Information about Business Customers and others (usually not considered "personal information"):

- ☐ Not applicable
- ☐ Name of business contact/firm representative, customer, and/or others
- ☐ Race/Ethnicity
- ☐ Gender
- ☐ Full or partial SSN:

- ☐ Business/corporate purpose(s)
- ☐ Other business/employment/job description(s)
- ☐ Professional affiliations
- ☐ Intra-business office address (office or workstation)
- ☐ Business telephone number(s)
- ☐ Business cell phone number(s)
- ☐ Business fax number(s)
- ☐ Business e-mail address(es)
- ☐ Bill payee name
- ☐ Bank routing number(s)
- ☐ Income/Assets
- ☐ Web navigation habits
- ☐ Commercially obtained credit history data
- ☐ Commercially obtained buying habits
- ☐ Personal clubs and affiliations
- ☐ Credit card number(s)
- ☐ Bank account(s)
- ☐ Other information:

1.10 Under the *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, Federal agencies are required to have a System of Records Notice (SORN) for an information system like this one, which contains information about individuals, *e.g.*, "personally identifiable information" (PII).

A System of Records Notice (SORN) is a description of how the information system will collect, maintain, store, and use the personally identifiable information (PII).

Does a SORN cover the PII in this information system?

- ☒ Yes
- ☐ No

If yes, what is this SORN: E-Filing/Case Management System

Please provide the citation that was published in the *Federal Register* for the SORN: 81 Fed. Reg. 44,335 (July 7, 2016)

Section 2.0 System of Records Notice (SORN):

2.1 What is the Security Classification for the information in this SORN, as determined by the OSHRC Security Officer?

There is no security classification.

2.2 What is the location of the information covered by this SORN?

Electronic records are maintained in a private cloud within an Oracle Database, operated by MicroPact at 12901 Worldgate Drive, Suite 800, Herndon, VA 20170.

2.3 What are the categories of individuals in the system of records covered by this SORN?

This system of records covers (1) administrative law judges; (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.

2.4 What are the categories of records[3] covered by this SORN?

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.

2.5 Under what legal authority(s) does the OSHRC collect and maintain the information covered by this SORN?

29 U.S.C. § 661

2.6 What are the purposes for collecting, maintaining, and using the information covered by this SORN?

This system of records is maintained for the purpose of processing cases that are before OSHRC.

2.7 What are the Routine Uses under which disclosures are permitted to "third parties," as noted in this SORN?

☒ Adjudication and litigation: Blanket Routine Use 1 (Attached).
☒ Court or Adjudicative Body: Blanket Routine Use 1 (Attached).
☐ Committee communications:
☐ Compliance with welfare reform requirements:
☐ Congressional inquiries: Blanket Routine Use 9 (Attached).
☐ Contract services, grants, or cooperative agreements:
☐ Emergency response by medical personnel and law enforcement officials:
☒ Employment, security clearances, licensing, contracts, grants, and other benefits by OSHRC: Blanket Routine Use 3 (Attached).
☒ Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*: Blanket Routine Use 4 (Attached).
☐ OSHRC enforcement actions:
☐ Financial obligations under the Debt Collection Act:
☐ Financial obligations required by the National Finance Center:
☐ First responders, *e.g.*, law enforcement, DHS, FEMA, DOD, NTIA, *etc.*:
☒ Government-wide oversight by NARA, DOJ, and/or OMB: Blanket Routine Uses 8, 10, and 12 (Attached).
☒ Labor relations: Blanket Routine Use 5 (Attached).
☒ Law enforcement and investigations: Blanket Routine Use 2 (Attached).
☐ National security and intelligence matters:
☒ Department of State, Department of Homeland Security, and other Federal agencies: Blanket Routine Use 6 (OPM, Attached).
☐ Program partners, *e.g.*, WMATA:
☒ Breach of Federal data: Blanket Routine Use 11 (Attached).

[3] This refers to the types of information that this information system or database collects, uses, stores, and disposes of when no longer needed.

☒ Others Routine Use disclosures not listed above:

- Records may be referred to a bar association or similar federal, state, or local licensing authority for a possible disciplinary action.
- Records may be disclosed to vetted MicroPact employees in order to ensure that the e-filing/case management system is properly maintained.
- In accordance with 29 U.S.C. § 661(g), OSHRC's case files may be disclosed to the public for the purpose of inspecting and/or copying the records at OSHRC.
- Blanket Routine Use 7 (Attached): Records may be disclosed 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.

2.8 What is the OSHRC's policy concerning whether information covered by this SORN is disclosed to consumer reporting agencies?

Disclosure is not permitted.

2.9 What are the policies and/or guidelines for the storage and maintenance of the information covered by this SORN?

At MicroPact's secure facility, the information is stored in a database contained on a separate database server behind the application server serving the data.

2.10 How is the information covered by this SORN retrieved or otherwise accessed?

Electronic records contained in the 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.

2.11 What are the safeguards that the system manager has in place to protect unauthorized access to the information covered by this SORN?

Data going across the Internet is encrypted using SSL encryption. Every system is password protected. MicroPact, which stores the data in a private cloud within an Oracle Database, operates its own data center that is protected by physical security measures. Only authorized MicroPact employees who have both physical key and key card access to the data center can physically access the sites where data is stored. Only authorized and vetted MicroPact employees have access to the servers containing any PII.

The access of parties and their representatives to electronic records in the e-filing 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.

2.12 What is the records retention and disposition schedule for the information covered by this SORN?

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.

2.13 What are the sources for the information in the categories of records covered by this SORN?

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.

Section 3.0 Development, Management, and Deployment and/or Sharing of the Information:

3.1 Who will develop the information system(s) covered by this SORN?

☐ Developed wholly by OSHRC staff employees:
☒ Developed wholly by OSHRC contractors: MicroPact
☐ Developed jointly by OSHRC employees and contractors:
☐ Developed offsite primarily by non-OSHRC staff:
☐ COTS (commercial-off-the-shelf-software) package:
☐ Other development, management, and deployment/sharing information arrangements:

3.2 Where will the information system be housed?

☐ OSHRC Headquarters
☐ American Eagle (web-site)
☒ MicroPact (case tracking system)
☐ Other information:
☐ Other information:

3.3 Who will be the primary manager(s) of the information system, *i.e.*, who will be responsible for assuring access to, proper use of, and protecting the security and integrity of the information?

(Check all that apply and provide a brief explanation)

☒ OSHRC staff in this bureau/office exclusively: OSHRC's IT department works with MicroPact to ensure information is properly safeguarded from outside incursions.
☐ OSHRC staff in other bureaus/offices:
☒ Information system administrator/Information system developers: OSHRC's IT department is the system administrator, and MicroPact is the developer
☒ Contractors: MicroPact
☐ Other information system developers, *etc*:

3.4 What are the OSHRC's policies and procedures that the information system's administrators and managers use to determine who gets access to the information in the system's files and/or database(s)?

The e-filing system relies on user roles to determine what files and/or database(s) a user may access.

3.5 How much access will users have to data in the information system(s)?

☐ Access to all data:
☒ Restricted access to data, as determined by the information system manager, administrator, and/or developer:
☐ Other access policy:

3.6 Based on the Commission policies and procedures, which user group(s) may have access to the information at the OSHRC:

(Check all that apply and provide a brief explanation)

☒ Information system managers:

☒ Information system administrators:
☒ Information system developers: MicroPact, for purpose of ensuring that the e-filing/case management system is properly maintained.
☒ OSHRC staff in this bureau/office: National office, extent of access depends on the user's role
☐ OSHRC staff in other bureaus/offices:
☒ OSHRC staff in other bureaus/offices in OSHRC field offices: National office, extent of access depends on the user's role
☒ Contractors: MicroPact (see above)
☒ Other Federal agencies: Department of Labor, access is limited to documents/information in cases where DOL is a party
☐ State and/or local agencies:
☐ Businesses, institutions, and other groups:
☐ International agencies:
☒ Individuals/general public: Access is limited to documents/information in cases where the individual is a party or representative of a party. The public has the right to inspect case files under section 12(g) of the OSH Act, 29 U.S.C. § 661(g), but will not be allowed direct electronic access to case files or other information in the information system. Case files contained in this information system, however, may be copied by an OSHRC employee and provided to the public pursuant to a FOIA request under 5 U.S.C. § 552, or for inspection under section 12(g) of the OSH Act.
☐ Other groups:

If contractors do not have access to the PII in this system, please skip to Question 3.9.

3.7 What steps have been taken to ensure that the contractors who have access to and/or work with the PII in the system are made aware of their duties and responsibilities to comply with the requirements under subsection (m) "Contractors" of the Privacy Act, as amended, 5 U.S.C. 552a(m)?

For any future contract with MicroPact or any other contractor maintaining an information system for the Commission, responsible agency personnel will ensure that the wording of the contract makes the provisions of the Privacy Act binding on the contractor and its employees.

3.8 What steps have been taken to insure that any Section M contract(s) associated with the information system covered by this SORN include the required FAR clauses (FAR 52.224-1 and 52.224-2)?

For any future contract with MicroPact or any other contractor maintaining an information system for the Commission, responsible agency personnel will ensure that the wording of the contract includes the required FAR clauses (FAR 52.224-1 and 52.224-2).

If there are no information linkages, sharing, and/or transmissions, please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.9 If the information system has links to other information systems (or databases), *i.e.*, it shares, transmits, or has other linkages, with what other non-OSHRC organizations, groups, and individuals will the information be shared?

(Check all that apply and provide a brief explanation)
☐ Other Federal agencies:

☐ State, local, or other government agencies:
☐ Businesses:
☐ Institutions:
☐ Individuals:
☐ Other groups:

Please explain your response:

3.10 If this information system transmits or shares information, including PII, between any other OSHRC systems or databases, is the other system (or database) covered by a PIA?

☐ Yes
☐ No

Please explain your response:

3.11 Since this information system transmits/shares PII between the OSHRC computer network and another non-OSHRC network, what security measures or controls are used to protect the PII that is being transmitted/shared and to prevent unauthorized access during transmission?

If there is no "matching agreement," *e.g.*, *Memorandum of Understand (MOU), etc*., please skip to **Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:**

3.12 What kind of "matching agreement," *e.g.*, *Memorandum of Understanding (MOU), etc.*, as defined by 5 U.S.C. 552a(u) of the Privacy Act, as amended, is there to cover the information sharing and/or transferred with the external organizations?

3.13 Is this a new or a renewed matching agreement?

☐ New matching agreement
☐ Renewed matching agreement

Please explain your response:

3.14 Has the matching agreement been reviewed and approved (or renewed) by the OSHRC's Data Integrity Board, which has administrative oversight for all OSHRC matching agreements?

☐ Yes; if yes, on what date was the agreement approved:
☐ No

Please explain your response:

3.15 Is the information that is covered by this SORN, which is transmitted or disclosed with the external organization(s), comply with the terms of the *MOU* or other "matching agreement?"

3.16 Is the shared information secured by the recipient under the *MOU*, or other "matching agreement to prevent potential information breaches?"

Section 4.0 Data Quality, Utility, Objectivity, and Integrity Requirements:

OMB regulations require Federal agencies to ensure that the information/data that they collect and use meets the highest possible level of quality and integrity. It is important, therefore, that the information the Commission's information systems use meets the "benchmark standards" established for the information.

4.1 How will the information that is collected from OSHRC sources, including OSHRC employees

and contractors, be checked for accuracy and adherence to the Data Quality guidelines?

(Please check all that apply)

☐ Information is processed and maintained only for the purposes for which it is collected.
☐ Information is reliable for its intended use(s).
☐ Information is accurate.
☐ Information is complete.
☐ Information is current.
☒ Not applicable:

Please explain any exceptions or clarifications:

OSHRC's Data Quality Guidelines, http://www.oshrc.gov/quality/quality.html, do not apply to information included in the e-filing system. Specifically, OSHRC notes the following in its guidelines:

> Consistent with OMB guidelines, these procedures do not apply to the dissemination of information relating to adjudicative processes, "such as the findings and determinations that an agency makes in the course of adjudications involving specific parties." 67 FR 8452, 8460 (February 22, 2002). The agency agrees with OMB's response, stated in the Federal Register, that there are "well established procedural safeguards and rights to address the quality of adjudicatory decisions and to provide persons with an opportunity to contest decisions." Id. Excluded categories of information include, but are not limited to, decisions, orders, opinions, subpoenas, adjudicative processes, amicus, and other briefs. Therefore, the agency will not impose additional requirements during the adjudicative proceedings or establish additional rights of challenge or appeal through this administrative procedure.

The e-filing system does contain some other information, such as registration, contact and/or user information pertaining to the parties, as well as agency personnel involved in the cases, such as administrative law judges and those processing the documents. But this information is not disseminated to the public, as "dissemination" is defined in OSHRC's guidelines. The guidelines, therefore, are not applicable.

If the Data Quality Guidelines do not apply to the information in this information system (or database), please skip to **Section 5.0 Safety and Security Requirements:**

4.2 If any information collected from non-OSHRC sources, how will the information sources be checked for accuracy and adherence to the Data Quality guidelines?

(Please check all that apply and provide an explanation)

☐ Yes, information is collected from non-OSHRC sources: Information is processed and maintained only for the purposes for which it is collected:
☐ Information is reliable for its intended use(s):
☐ Information is accurate:
☐ Information is complete:
☐ Information is current:
☐ No information comes from non-OSHRC sources:

Please explain any exceptions or clarifications:

If the information that is covered by this SORN is not being aggregated or consolidated, please skip to Question 4.5.

4.3 If the information that is covered by this system of records notice (SORN) is being aggregated or consolidated, what controls are in place to ensure that the information is relevant, accurate, and complete?

4.4 What policies and procedures do the information system's administrators and managers use to ensure that the information adheres to the Data Quality guidelines both when the information is obtained from its sources and when the information is aggregated or consolidated for the use by the bureaus and offices?

4.5 How often are the policies and procedures checked routinely—what type of annual verification schedule has been established to ensure that the information that is covered by this SORN adheres to the Data Quality guidelines?

Section 5.0 Safety and Security Requirements:

5.1 How are the records/information/data in the information system or database covered by this SORN stored and maintained?

☒ IT database management system (DBMS)
☐ Storage media including CDs, CD-ROMs, *etc*.
☐ Electronic tape
☐ Paper files
☐ Other:

5.2 Is the information collected, stored, analyzed, or maintained by this information system or database available in another form or from another source (other than a "matching agreement" or *MOU*, as noted above)?

☒ Yes
☐ No

Please explain your response:

Case files are also maintained in paper form.

5.3 What would be the consequences to the timely performance of OSHRC's operations if this information system became dysfunctional?

E-file users would have to resort to other methods of filing (mail, fax, or personal delivery, *see* 29 CFR § 2200.8(c)) if they were unable to file via the e-filing system. But deadlines for filing documents with the Commission would likely remain the same, to the extent that administrative law judges or the Commission found no bases to grant extensions. Similarly, if administrative law judges were unable to issue orders through the e-filing system, these same alternative methods could be used. If the e-filing system became dysfunctional, OSHRC and the parties would certainly be inconvenienced, but any delays to the adjudicatory process would be minimal.

5.4 What will this information system do with the information it collects:

☐ The system will create new or previously unavailable information through data aggregation, consolidation, and/or analysis, which may include information obtained through link(s), sharing, and/or transferred to/from other information systems or databases;
☒ The system collects PII, but it will not perform any analyses of the PII data.

Please explain your response:

The information is collected only to allow OSHRC to process cases that come before the administrative law judges and the Commission.

5.5 Will the OSHRC use the PII that the information system (or database) collects to produce reports on these individuals?

☐ Yes
☒ No

Please explain your response:

The information is collected only to allow OSHRC to process cases that come before the administrative law judges and the Commission.

5.6 What will the system's impact(s) be on individuals from whom it collects and uses their PII:

☐ The information will be included in the individual's records;
☐ The information will be used to make a determination about an individual;
☒ The information will be used for other purposes that have few or no impacts on the individuals.

Please explain your response (including the magnitude of any impact[s]):

The information is collected only to allow OSHRC to process cases that come before the administrative law judges and the Commission.

5.7 Do individuals have the right to the following?

They may decline to provide their PII?

☒ Yes
☐ No

They may consent to particular uses of their PII?

☒ Yes
☐ No

Please explain your response(s) (including the potential consequences for refusing to provide PII):

Use of the e-filing system is optional. To the extent that a party does not wish to enter his or her personal data into the e-filing system, other methods for filing documents under 29 CFR § 2200.8(g) remain available. Certain information about the parties, however, must be maintained in order for the adjudicative process to function properly. In accordance with 29 CFR § 2200.6, regardless of the method of filing, "[e]very pleading or document filed by any party or intervenor shall contain the name, current address and telephone number of his representative or, if he has no representative, his own name, current address and telephone number."

If individuals do not have the right to consent to the use of their information, please skip to Question 5.10.

5.8 If individuals have the right to consent to the use of their PII, how does the individual exercise this right?

If the individual is a litigant before the Commission, the party (or its representative) can opt not to use the e-filing system.

5.9 What processes are used to notify and to obtain consent from the individuals whose PII is being collected?

If the individual is a litigant before the Commission, the party (or its representative) can opt not to use the e-filing system. Thus, by using the system and entering personal information, the user is consenting to collection of that data. Before the user enters the system and data is collected, a privacy notice is displayed, providing the user with information concerning how the data may be used.

5.10 How will the information be collected and/or input into this information system (or database):

(Choose all the apply)

☒ The information system has a link to the OSHRC's Internet address at www.OSHRC.gov or other customer-facing URL;
☐ The information system has a customer-facing web site via the OSHRC Intranet for OSHRC employees;
☐ The information is collected from the individual by fax;
☐ The information is collected from the individual by e-mail;
☐ The information is collected from the individual by completing an OSHRC form, license, and/or other document;
☐ The information is collected from the individual by regular mail; and/or
☐ The information concerning individuals is collected by other methods.

Please explain your response:

The information system is accessible on www.OSHRC.gov via a button, titled "OSHRC E-Filing System" and linked to the URL for the e-filing system.

5.11 How does this system advise individuals of their privacy rights when they submit their PII?

☐ The system contains a link to the OSHRC's privacy policies for all users at the OSHRC's website www.OSHRC.gov:
☒ A Privacy Notice is displayed on the webpage:
☐ A Privacy Notice is printed at the end of the OSHRC form(s), license(s), and/or other Commission document(s): HRM collects information directly from OSHRC employees when they submit their bi-weekly payroll and leave data.
☐ The OSHRC Intranet site displays a Privacy Notice:
☐ The collection or input mechanism uses another method to provide individuals with the Privacy Notice:
☐ No Privacy Notice is provided:

5.12 If a Privacy Notice is provided, which of the following are included?

☒ Proximity and timing—the privacy notice is provided at the time and point of data collection.
☐ Purpose—describes the principal purpose(s) for which the information will be used.
☐ Authority—specifies the legal authority that allows the information to be collected.
☐ Conditions—specifies whether providing the information is voluntary, and the effects, if any, of not providing it.
☒ Disclosures—specify the routine use(s) that may be made of the information.
☐ Not applicable, as information will not be collected in this way.

Please explain your response:

The Privacy Notice is provided immediately before the user enters the system. The notice provides the more general disclosures pertaining to law enforcement, but the other, more specific

routine uses are set forth in the applicable system of records notice, https://www.federalregister.gov/documents/2016/07/07/2016-16065/privacy-act-of-1974-revised-system-of-records.

5.13 Will consumers have access to information and/or the information system on-line via www.OSHRC.gov?

☒ Yes
☐ No

Please explain your response:

The information system is accessible on www.OSHRC.gov via a button, titled "OSHRC E-Filing System" and linked to the URL for the e-filing system. To the extent that a party in a case before OSHRC is considered a "consumer," the party will have limited access to information in the information system. The party's access will be limited based on that party's user role.

5.14 What safeguards and security measures, including physical and technical access controls, are in place to secure the information and to minimize unauthorized access, use, or dissemination of the information that is stored and maintained in the information system?

(Check all that apply)

☒ Account name
☒ Passwords
- ☐ Accounts are locked after a set period of inactivity
- ☐ Passwords have security features to prevent unauthorized disclosure, *e.g.*, "hacking"
- ☒ Accounts are locked after a set number of incorrect attempts
- ☐ One time password token
- ☐ Other security features:

☒ Firewall
☐ Virtual private network (VPN)
☒ Data encryption:
☒ Intrusion detection application (IDS)
☐ Common access cards (CAC)
☐ Smart cards:
☐ Biometrics
☐ Public key infrastructure (PKI)
☐ Locked file cabinets or fireproof safes
☒ Locked rooms, with restricted access when not in use
☐ Locked rooms, without restricted access
☐ Documents physically marked as "sensitive"
☐ Guards
- ☐ Identification badges
- ☐ Key cards
- ☐ Cipher locks
- ☐ Closed circuit TV (CCTV)

☐ Other:

5.15 Please explain what staff security training and other measures are in place to assure that the security and privacy safeguards are maintained adequately?

Each OSHRC employee is required to complete Privacy Act and Security training annually.

5.16 How often are the security controls reviewed?

☒ Six months or less
☐ One year
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☐ Other:

5.17 How often are ITC personnel (*e.g.*, information system administrators, information system/information system developers, contractors, and other ITC staff, *etc*.) who oversee the OSHRC network operations trained and made aware of their responsibilities for protecting the information?

☐ There is no training
☒ One year
☐ Two years
☐ Three years
☐ Four years
☐ Five years
☐ Other:

If privacy training is provided, please skip to Question 5.19. Mandatory privacy training is provided annually.

5.18 What are the safeguards to ensure that there are few opportunities for disclosure, unavailability, modification, and/or damage to the information system covered by this SORN, and/or prevention of timely performance of OSHRC operations if operational training is not provided?

5.19 How often must staff be "re-certified" that they understand the risks when working with personally identifiable information (PII)?

☐ Less than one year
☒ One year
☐ Two years
☐ Three or more years
☐ Other re-certification procedures:

5.20 Do OSHRC's training and security requirements for this information system conform to the requirements of the Federal Information Security Modernization Act (FISMA)?

☒ Yes
☐ No

Please explain your response:

A breach notification policy is in place, and specific to this information system, a PTA was conducted, which in turn necessitated the current PIA, and a revised SORN was issued. Additionally, security training, as well as Privacy Act training, is provided annually to all OSHRC employees.

If the Privacy Threshold Assessment (PTA) was completed recently as part of the information system's evaluation, please skip Questions 5.21 through 5.24, and proceed to Question 5.25.

5.21 What is the potential impact on individuals on whom the information is maintained in the information system(s) if unauthorized disclosure or misuse of information occurs?

(Check one)

☐ Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual.
☐ Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual.
☐ Results in significant harm, embarrassment, inconvenient, or unfairness to the individual.

Please explain your response:

5.22 What is the impact level for the information system(s) covered by this SORN and is it consistent with the guidelines as determined by the FIPS 199 assessment?

5.23 When was the "Assessment and Authorization" (A&A) completed for the information system(s) covered this SORN—please provide the A&A completion date?

5.24 Has the Chief Information Officer (CIO) and/or the Chief Information Security Officer (CISO) designated this information system as requiring one or more of the following:

☐ Independent risk assessment:
☐ Independent security test and evaluation:
☐ Other risk assessment and/or security testing procedures, *etc.*:
☐ Not applicable:

5.25 Does this information system use technology in ways that the Commission has not done so previously, *i.e.*, Smart Cards, Caller-ID, etc.?

OSHRC has migrated from an in-house managed case tracking system to a FedRAMP certified cloud-based solution that allows litigants to file pleadings electronically.

5.26 How does the use of the technology affect the privacy of the general public and OSHRC employees and contractors?

OSHRC requires individuals to provide only limited PII so that cases can be effectively processed.

5.27 Does this information system (covered by this SORN) include a capability to identify, locate, and/or monitor individuals?

☐ Yes
☒ No

If the information system does not include any monitoring capabilities, please skip to **Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):**

5.28 If the information system includes the technical ability to monitor an individual's movements identified in Questions 5.25 through 5.27 above, what kinds of information will be collected as a function of the monitoring of individuals?

5.29 What controls, policies, and procedures, if any, does this information system (covered by this SORN) contain any controls, policies, and procedures to prevent unauthorized monitoring?

Section 6.0 Information Collection Requirements under the Paperwork Reduction Act (PRA):

If this information system or database affects only OSHRC employees, please skip to Section 9.0

6.1 Does the information system or database covered by this SORN solicit information via paperwork and/or recordkeeping requirements that effect the general public (non-OSHRC employees), which may include any of the following (including both voluntary and required compliance):

☐ OSHRC forms, licenses, or other documentation;
☐ Participation in marketing, consumer, or customer satisfaction surveys or questionnaires;
☐ Recordkeeping or related activities.

If so, is this information system subject to the requirements of the PRA because it solicits information via paperwork and/or recordkeeping requirements

☐ Yes, the information system includes any paperwork and/or recordkeeping requirements that non-OSHRC employees and contractors must complete.
☒ No, the information system does impose any paperwork and/or recordkeeping requirements, *i.e.*, the information it collects does not constitute an "information collection" as defined by the PRA.

If there are no paperwork or recordkeeping requirements (or if only OSHRC employees and contractors are the effected groups), this information system is exempt from the requirements of the PRA. Please skip to **Section 7.0 Correction and Redress:**

6.2 Is there a website that requests information, such as the information necessary to complete an OSHRC form, license, authorization, *etc*.?

☐ Yes
☐ No or Not applicable

Please explain your response:

6.3 If there are one or more PRA information collections that are covered by this SORN that are associated with the information system's databases and paper files, please list the OMB Control Number, Title of the collection, and Form number(s) as applicable for the information collection(s):

6.4 Are there are any OSHRC forms associated with the information system(s) covered by this SORN, and if so, do the forms carry the Privacy Act notice?

☐ Yes:
☐ No
☐ Not applicable—the information collection does not include any forms.

6.5 Have the system managers contacted the Performance Evaluation and Records Management (PERM) staff to coordinate PRA requirements and submission of the information collection to the Office of Management and Budget?

☐ Yes
☐ No

Please explain your response:

Section 7.0 Correction and Redress:

7.1 What are the procedures for individuals wishing to inquire whether this SORN contains information about them consistent with OSHRC's Privacy Act rules under 29 CFR part 2400?

Such inquiries should be addressed to the 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 § 2400.5 (notification), and 29 CFR § 2400.6 (procedures for requesting records).

7.2 What are the procedures for individuals to gain access to their own records/information/data in this information system that is covered by this SORN consistent with OSHRC's Privacy Act rules under 29 CFR part 2400?

Such requests should be addressed to the 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 § 2400.6 (procedures for requesting records).

7.3 What are the procedures for individuals seeking to correct or to amend records/information/data about themselves in the information system that is covered by this SORN consistent with OSHRC's Privacy Act rules under 29 CFR part 2400?

Such requests should be addressed to the Privacy Officer, OSHRC, 1120 20th Street NW, Ninth Floor, Washington, DC 20036-3457. For an explanation on the specific procedures for contesting the contents of a record, refer to 29 CFR § 2400.8 (Procedures for requesting amendment), and 29 CFR § 2400.9 (Procedures for appealing).

7.4 Does this SORN claim any exemptions to the notification, access, and correction, and/or amendment procedures as they apply to individuals seeking information about them in this SORN, and if so, are these exemptions consistent with OSHRC's Privacy Act rules under 29 CFR part 2400?

No.

7.5 What processes are in place to monitor and to respond to privacy and/or security incidents? (Please specify what is changing if this is an existing SORN that is being updated or revised?)

Safeguards described above and in the SORN are in place to minimize the potential of a privacy and/or security incident. If one does occur, OSHRC has a breach policy in place that requires any employee recognizing that a breach has (or may have) occurred to notify appropriate agency personnel so that any necessary corrective action can be taken.

7.6 How often is the information system audited to ensure compliance with OSHRC and OMB regulations and to determine new needs?

☐ Six months or less
☒ One year
☐ Two years
☐ Three years:
☐ Four years
☐ Five years
☐ Other audit scheduling procedure(s):

Section 8.0 Consumer Satisfaction:

8.1 Is there a customer or consumer satisfaction survey included as part of the public access to the

information covered by this information system or database?

☐ Yes
☐ No
☒ Not applicable

Please explain your response:

If there are no Consumer Satisfaction requirements, please skip to **Section 9.0 Risk Assessment and Mitigation:**

8.2 Have any potential Paperwork Reduction Act (PRA) issues been addressed prior to implementation of the customer satisfaction survey?

☐ Yes
☐ No

Please explain your response:

Section 9.0 Risk Assessment and Mitigation:

9.1 What are the potential privacy risks for the information covered by this system of records notice (SORN), and what practices and procedures have you adopted to minimize them?

Risks:	Mitigating factors:
a. PII—mostly contact data—is entered into the electronic system.	a. For the most part, those using the e-filing system enter their own contact data, increasing the likelihood that the data is accurate. As to the potential for an unauthorized release of information, safeguards described above and in the SORN are in place to minimize the likelihood of such a release. Additionally, OSHRC has a breach policy in place to mitigate damage caused by any incursion into the system.

9.2 What is the projected production/implementation date for the information system(s) or database(s):

Initial implementation: 9/2016
Secondary implementation: N/A
Tertiary implementation: N/A
Other implementation: N/A

9.3 Are there any ancillary and/or auxiliary information system(s) or database(s) linked to this information system that are covered by this SORN, which may also require a Privacy Impact Assessment (PIA)?

☐ Yes
☒ No

If so, please state the application(s), if a Privacy Impact Assessment (PIA) has been done, and the completion date for PIA: