Occupational Safety and Health Review Commission

Privacy Impact Assessment (PIA)

Information System: Occupational Safety and Health Review Commission Network and General Support System

Component: oshrc.gov

Date: 02/7/2025

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

Section 1.0 Information System's Contents:

1.1 Action necessitating Privacy Impact Assessment (PIA):

☐ New information system—**Implementation date:**
☒ Revised or upgraded information system—**Revision or upgrade date:** February 2025

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:

☐ New collection of information—**Collection date:**

Through OSHRC's website, oshrc.gov, members of the public may subscribe to "E-Alerts," a service which provides updates via the individual's email when new information is posted on the website, including Commission and ALJ decisions and documents on the Open Government web page. This information system component maintains a listing of the names of individuals who subscribe to this service and their email addresses. Based on the results of a Privacy Threshold Assessment (PTA), conducted on August 5, 2019, the SAOP and CIO determined that a Privacy Impact Analysis (PIA) was warranted, which was subsequently conducted.

The agency's website is being updated again in February 2025. The E-Alerts subscription service has not changed. However, OSHRC's Decision Search webpage has been revised to allow for searches via case name (which could include sole proprietors), docket number, and keyword search (which include individuals named in the decisions). In addition, the ability to submit FOIA requests through the website has been added. These online submissions may contain names, residential addresses, email addresses, and personal telephone numbers, as well as any other personal information that FOIA requesters enter into an open field to describe their requests. These submissions are converted into a pdf, which is then emailed to the agency's dedicated FOIA email account. However, information from the FOIA request submissions is also maintained on the website's server for 120 days before being automatically deleted. Based on the results of a PTA conducted on February 7, 2025, the SAOP and the CIO have determined that reevaluation of the website's PIA is warranted.

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

☒ Yes
Date: August 13, 2019, revised October 1, 2021, and February 7, 2025.

☐ 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** **(The PTA is attached.)**

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

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: The information collected from E-Alerts subscribers was previously addressed in a revision to the following SORN: Database of Commission and ALJ Decisions, and Other Case-Related Documents, on OSHRC Website, OSHRC-8. A revised SORN, which addresses changes to the website and includes the information described below, will soon be submitted to the Office of Information and Regulatory Affairs for review.

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? The information covered by the SORN is unclassified.

2.2 What is the location of the information covered by this SORN? OSHRC's website is hosted by WP Engine, and records from the website are stored within Google Cloud Platform's data center in Council Bluffs, Iowa.

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

This system of records covers all individuals referenced and described in Commission and ALJ decisions, and other case-related documents posted on OSHRC's website, including sole proprietors who were cited by OSHA, employees and other witnesses, attorney and non-attorney representatives of each party, and the Commissioners and ALJs. This system also covers individuals who subscribe to "E-Alerts" on the website, as well as individuals who submit FOIA requests through the website.

2.4 What are the categories of records[1] covered by this SORN?

This system of records includes final decisions issued by the Commission since 1972, and final decisions issued by the ALJs since 1993. This system also includes documents posted on OSHRC's Open Government webpage, including select orders issued by ALJs and the Commission, briefing notices issued since 2010, listings of new cases received since 2010, and monthly docket reports issued since 2010. In addition, this system includes certain documents posted in OSHRC's e-FOIA Reading Room, including case filings in select Commission cases. The documents may contain the following information: (1) the names and locations (city and state) of the individuals representing each party; (2) the names of sole proprietors cited by OSHA, as well as employees and other witnesses, and information describing those individuals, including job title and duties, medical history, and other descriptive information that is relevant to the disposition of a case; and (3) the names and job titles of the Commissioners and ALJs. This system also includes a database that contains the names and email addresses of those individuals who subscribe to "E-Alerts." Finally, this system includes a database for submission of online FOIA requests, which may contain names, residential addresses, email addresses, and personal telephone numbers, as well as any other personal information that FOIA requesters enter into an open field to describe their requests.

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

5 U.S.C. 552; 29 U.S.C. 661(g); OMB Memorandum M-10-06; OMB Memorandum M-16-16; OMB Memorandum M-23-22; OMB Memorandum M-24-08.

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

This system of records is maintained in order to make Commission and ALJ decisions, as well as other case-related documents, more accessible to the public and agency employees, and to allow for online submission of Freedom of Information Act (FOIA) requests.

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

☒ Adjudication and litigation: Routine Use 1.
☒ Court or Adjudicative Body: Routine Use 1.
☐ Committee communications:
☐ Compliance with welfare reform requirements:
☒ Congressional inquiries: Routine Use 9.
☐ 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: Routine Use 3.

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

☒ Employment, security clearances, licensing, contracts, grants, and other benefits upon a request from another Federal, state, local, tribal, or other public authority, *etc.*: Routine Use 4.
☐ 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, OPM, and/or OMB: Routine Uses 6, 8, 10, and 12.
☒ Labor relations: Routine Use 5.
☒ Law enforcement and investigations: Routine Use 2.
☐ National security and intelligence matters:
☒ Department of State, Department of Homeland Security, and other Federal agencies: Routine Use 7.
☐ Program partners, *e.g.*, WMATA:
☒ Breach of Federal data: Routine Uses 11 and 13.
☒ Others Routine Use disclosures not listed above:

- **Routine Use 14:** This system of records is maintained in order to make Commission and ALJ decisions, as well as other case-related documents, more accessible to the public and agency employees.

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

Disclosure to consumer reporting agencies is not permitted.

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

Records are stored by WP Engine within Google Cloud Platform's data center in Council Bluffs, Iowa. OSHRC requests updates for its website through a secure portal. The website's records are secured within Google Cloud Platform's data center in accordance with federal standards. Access to the names and email addresses of those who subscribe to "E-Alerts," as well as information submitted through the online FOIA forms, is limited to OSHRC system administrators.

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

Commission and ALJ decisions on OSHRC's website can be retrieved by case name, docket number, or keyword search via the search engine located on the website's Decision Search page, and all other documents maintained on the website can be retrieved by a simplified Boolean search via the search engine located on the website's homepage. Although not searchable on the website, the names and email addresses of those who subscribe to "E-Alerts" and information that FOIA requesters submit through the website can be retrieved by OSHRC system administrators.

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

Records are retained and disposed of in accordance with OSHRC Records Control Schedule N1-455-11-003. Pursuant to General Records Schedule 5.1, Item 20, records from FOIA Requests submissions are maintained within Google Cloud Platform's data center for 120 days for business use and then automatically deleted.

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

Information in this system of records is derived from records associated with contested cases

adjudicated before the Commission and/or the ALJs and, thus, the information may come from individuals who are the subjects of the records or from other sources. Information also comes from individuals who subscribe to "E-Alerts" or submit FOIA requests through the website.

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:
☒ 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
☒ Google Cloud Platform (website)
☐ Tyler Federal, LLC (case tracking system)
☐ Office 365
☐ 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?

☒ OSHRC staff in this bureau/office
☐ OSHRC staff in other bureaus/offices
☒ Website host
☐ 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 Commission's website, oshrc.gov, is a public website. The public, therefore, has access to all information posted on the website. Access to the names and email addresses of those who subscribe to E-Alerts, as well as any PII that is included in a FOIA request submission, is limited to OSHRC system administrators, who require access to perform their work duties. Agency personnel who process FOIA requests will have access to the information included in those forms once they are converted into a pdf and emailed to the agency's dedicated FOIA account.

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: Information posted on oshrc.gov is available to the public, but access to the names and email addresses of E-Alerts subscribers, as well as PII from FOIA request submissions, is limited to OSHRC system administrators.
☐ 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:

Only OSHRC system administrators have access to the names and email addresses of E-Alerts

subscribers and PII from FOIA request submissions. All user groups have access to the information posted on oshrc.gov.

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)?

In the event a contractor works as an OSHRC system administrator, that individual must complete the same Privacy Act and security awareness training, when first hired and then annually thereafter, that OSHRC employees are required to complete.

3.8 What steps have been taken to ensure 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)?

OSHRC's policy is to include up-to-date FAR clauses in each section M contract.

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

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: (There are no matching agreements.)**

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?

The specific procedures for checking and maintaining the quality of information posted on oshrc.gov are specified in the agency's *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Disseminated Information & Procedures for the Public to Seek Correction of Disseminated Information*.

These procedures apply to information such as guides to agency procedures and agency reports. They do not apply, however, to some of the other information covered by this PIA, including ALJ and Commission decisions:

> 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, 8454 (Feb. 22, 2002). The agency agrees with OMB's statement 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, and briefs. Therefore, the agency will not impose additional requirements during its adjudicative proceedings or establish additional rights of challenge or appeal through this administrative procedure.

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: Some documents posted in the e-FOIA Reading Room are produced and submitted by parties during the adjudicative process. Other than redacting certain PII pursuant to the agency's redaction policy, these documents are not modified by the agency. As noted above, these documents are not subject to the Data Quality guidelines. Other documents posted on oshrc.gov are not collected from non-OSHRC sources.

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?

The accuracy of the SORNs is reviewed annually.

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: Records are stored and maintained within Google Cloud Platform's data center in Council Bluffs, Iowa.

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: Paper copies of case-related materials, including Commission and ALJ decisions, are maintained by the agency's Office of the Executive Secretary. These materials are also available, electronically, through OSHRC's e-filing system. Both of these sources are covered by the following SORN: E-Filing/Case Management System, OSHRC-6. In addition, electronic copies of FOIA request submissions are maintained by the Office of General Counsel and are covered by the following SORN: *Office of the General Counsel Records*, OSHRC-5.

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

If the information system component (oshrc.gov) became dysfunctional, OSHRC's various offices would still be able to perform their intended functions, as the offices' work product would not be affected. OSHRC staff relies primarily on the agency's local server to maintain work product (*see* PIA for LAN/WAN), as well as Office 365 (*see* PIA for Office 365) and the e-filing system (*see* PIA for EFS). Although the public's ability to access documents would be affected, such information could still be requested through the agency's Freedom of Information Act Requester Service Center.

Although the public's ability to submit FOIA requests online would be affected, other permissible submission options—mail, email, and fax—are also available. In addition, when a request is submitted through the agency website, an electronic copy of that request (converted to a pdf) is immediately sent to the agency's dedicated FOIA account. FOIA personnel, therefore, would not be affected if the data stored within Google Cloud Platform's data center could not be accessed.

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.

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

☐ Yes
☒ No

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 impact on the individuals from whom PII is collected is minimal because (1) the most sensitive PII is redacted from any documents that are posted on the website; (2) the E-Alerts subscribers' names and email addresses and PII from FOIA request submissions are provided voluntarily and can be accessed by only OSHRC system administrators (unless disclosed pursuant to a routine use); and (3) any information from FOIA request submissions is automatically deleted from Google Cloud Platform's data center within 120 days.

5.7 Do individuals have the right to the following?

They may decline to provide their PII?

☐ Yes

☒ No

Some of the PII covered by this PIA is included in filings from case records. Admission of these records into evidence and their use in the agency's adjudicative proceedings is generally not in the control of the PII's subject. Nonetheless, Commission procedural rules (29 C.F.R. § 2200.8(c)(6), (d)(5)) are in place to minimize the amount of PII that is in the record. And before such documents are posted on oshrc.gov, they are reviewed and redacted in accordance with 5 U.S.C. § 552(b)(6) and the Commission's redaction policy. Thus, the most sensitive PII from the case records is not included on oshrc.gov, the information system component at issue here.

PII from E-Alerts subscribers and FOIA requesters is provided voluntarily.

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): See 5.7 explanation.

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?

E-Alerts subscribers must provide their names and email addresses to receive updates. Individuals may opt not to sign up for the service. Certain PII from FOIA requesters is necessary for the agency to process their requests. However, FOIA requesters may opt to submit a FOIA request via mail, email, or fax, and are not required to submit their requests through the website.

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

The subscription process makes clear that a name and email address is required to subscribe to E-Alerts, and the FOIA request form makes clear that the information being collected is necessary for the agency to process the FOIA request. Both the E-Alerts and FOIA request forms include Privacy Act Statements.

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; FOIA requests can be submitted through an online FOIA form.
☐ 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 website's records are secured within Google Cloud Platform's data center in accordance with federal standards. Before any case-related documents are posted

on the website, OSHRC's privacy personnel review the documents and redact PII in accordance with the agency's redaction policy. E-Alerts subscribers and FOIA requesters may enter certain PII (discussed above) into online forms via oshrc.gov. Once entered, the information from the E-Alerts subscribers and the FOIA requesters can be accessed only by OSHRC system administrators.

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

A link to the privacy policy for oshrc.gov is in the website's footer and therefore appears at the bottom of each webpage. In addition, the following Privacy Act Statement appears on the webpage through which individuals subscribe to E-Alerts or submit online FOIA requests:

> Pursuant to 5 U.S.C. § 552a(e)(3), the following Privacy Act Statement serves to inform you that subscribing to E-Alerts will result in the collection of your name and email address. This information will be used only to provide E-Alerts to those who subscribe to the service, which is authorized under 5 U.S.C. § 552 and 29 U.S.C. § 661(g). You are voluntarily providing this information to the Review Commission and may withdraw your subscription at any time. Although the Review Commission does not anticipate further disclosing the information provided, it may be disclosed as indicated in the routine uses described in OSHRC-8, the applicable system-of-records notice published at 83 Fed. Reg. 62627 (Dec. 4, 2018).
>
> Pursuant to 5 U.S.C. § 552a(e)(3), the following Privacy Act Statement serves to inform you that completing this Freedom of Information Act (FOIA) Request Form will result in the collection of personally identifiable information (PII), which could include your name, home address, telephone number, and/or email address, as well as any PII entered into fields that require a description of your FOIA request or an explanation for any expedited processing or fee waiver request. This collection of information is authorized by the FOIA, 5 U.S.C. § 552, and the Review Commission's regulations implementing the FOIA, 29 C.F.R. pt. 2201. This information will be used to facilitate timely processing of your FOIA request. Any information you provide in this form is voluntary, but if you do not provide contact information, the Review Commission will not be able to process your FOIA request. The information collected through this FOIA Request Form may be disclosed in accordance with the routine uses specified in OSHRC-5, the applicable system-of-records notice, which is available on the Review Commission's privacy page.

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.

5.13 Will consumers have access to information and/or the information system on-line via

www.OSHRC.gov?

☒ Yes
☐ No

The public will have access to any information posted on the website, but only the OSHRC system administrators will have access to names and email addresses submitted by subscribers to E-Alerts and PII submitted by FOIA requesters through the online request form.

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? The following applies only to names and email addresses collected through the E-Alerts subscription process and PII collected through the FOIA request forms, as information posted on the website is publicly available.

(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 and contractor is required to complete Privacy Act and security awareness 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:

5.18 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:

5.19 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. Additionally, specific to oshrc.gov, PTAs and PIAs have been conducted, and the SORN covering the website has been revised, whenever there have been substantive changes to this system. Finally, security awareness training, as well as privacy training, is required annually for all OSHRC employees and contractors.

If the Privacy Threshold Assessment (PTA) was completed recently as part of the information system's evaluation, please skip **Questions 5.20 through 5.23**, and proceed to **Question 5.24**. **(The PTA is attached.)**

5.20 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:

5.21 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?

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

5.23 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:

5.24 Does this information system use technology in ways that the Commission has not done so previously, *i.e.*, Smart Cards, Caller-ID, etc.? No.

5.25 How does the use of the technology affect the privacy of the general public and OSHRC employees and contractors? Technology—through access restrictions and password requirements—protects the information collected from E-Alerts subscriptions and FOIA requests from unintended disclosure. Also, redaction technology protects PII in documents that are posted to oshrc.gov.

5.26 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).** **(The information system component does not include monitoring capabilities.)**

5.27 If the information system includes the technical ability to monitor an individual's movements identified in Questions 5.24 through 5.26 above, what kinds of information will be collected as a function of the monitoring of individuals?

5.28 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): No.

☐ 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. OMB's memorandum, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act" (Apr. 7, 2010), states that merely collecting names and email addresses, as is done for the E-Alerts subscription service, does not constitute "information collection" under the PRA. As to the FOIA requests submissions, the public is requesting information from the agency rather than the other way around, and the agency is simply attempting to ascertain facts that are necessary to process the request, which may not be considered "information" under the PRA; the online FOIA request form is provided as an option to the public for their convenience—there are other permissible options for submitting such requests—and therefore the form does not actually include "any requirement or request for persons to obtain, maintain, retain, report, or publicly disclose information." *See* 5 C.F.R. § 1320.3(c) (definition of "collection of information"), (h)(1) (definition of "information").

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**: **(PRA requirements do not apply here.)**

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 § 2400.4 (procedures for requesting notification of and access to personal 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 § 2400.4 (procedures for requesting notification of and access to personal 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 § 2400.6 (procedures for amending personal records), and 29 CFR § 2400.7 (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 SORNs are in place to minimize the potential of a privacy and/or security incident. If one does occur, OSHRC's breach policy 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**: **(There are no Consumer Satisfaction requirements.)**

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. Some case records containing PII are available to the public on the website's e-FOIA Reading Room.	1. The Commission's procedural rules (29 C.F.R. § 2200.8(c)(6), (d)(5)) minimize the amount of PII in documents that are admitted into evidence. 2. The Commission's redaction procedures limit the amount of PII that is disclosed to the public when documents are posted on the website.
b. Commission and ALJ decisions containing PII are available to the public on website.	1. The Commission and the ALJs typically draft decisions in a manner that eliminates or limits the inclusion of PII. 2. The Commission's redaction procedures limit the amount of PII that is disclosed to the public when documents are posted on the website.

Risks:	Mitigating factors:
c. Names and e-mail addresses of E-Alerts subscribers.	1. The list of names and emails is access-restricted to OSHRC system administrators.
d. PII from FOIA request submissions.	1. PII maintained within the data center is access-restricted to OSHRC system administrators. 2. Information collected through the online FOIA forms, including PII, is automatically deleted from the cloud within 120 days.

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

Initial implementation: Already implemented.
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 PIA?

☐ Yes
☒ No

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

Occupational Safety Health & Review Commission

Privacy Threshold Analysis (PTA)

Information System: Occupational Safety and Health Review Commission Network and General Support System

Component: oshrc.gov

Date: 08/13/2019, revised 10/1/2021 and 02/7/2025

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

Section 1.0 Information System's Status:

1.1 Status of the Information System:

☐ New information system—**Implementation date:**
☒ Revised or upgraded information system—**Revision or upgrade date:** February 2025

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:

As noted in prior PTAs, through OSHRC's website, members of the public may subscribe to "E-Alerts," a service which provides updates via email to the individual's email address when new information is posted on the website, including Commission and ALJ decisions and documents on the Open Government webpage. This system maintains a listing of the names of individuals who subscribe to this service and their email addresses.

As to the February 2025 update to the agency's website, OSHRC's Decision Search webpage has been revised to allow for searches via case name (which could include sole proprietors), docket number, and keyword search. In addition, the ability to submit FOIA requests through the website has been added. These online submissions may contain names, residential addresses, email addresses, and personal telephone numbers, as well as any other personal information that FOIA requesters enter into an open field to describe their requests. These submissions are converted to a pdf, which is then emailed to the agency's dedicated FOIA email account. Information from the FOIA request submissions is also maintained on the website's server for 120 days before being automatically deleted.

If this is a new information system, please skip to **Question 1.6**.

1.2 Has this information system existed under another name, or has the name been changed or modified?

☐ Yes
☒ No

Please explain your response:

1.3 Has this information system existed previously or been operated under any other software program, information system medium, *i.e.*, electronic database or paper files, and/or other format?

☐ Yes
☒ No

Please explain your response:

1.4 Has this information system existed under a system of records notice (SORN) by itself, or was it ever part or component of another SORN?

☒ Yes
☐ No

Please explain your response: The information maintained on oshrc.gov is covered by the SORN, OSHRC-8. Revisions to this SORN, which address changes to the website, will soon be submitted to the Office of Information and Regulatory Affairs for review.

1.5 Is this information system being changed or upgraded, and if so, what are the purposes for changing or upgrading the information system, and/or will any changes now include personally identifiable information (PII):

☒ Yes
☐ No

Please explain your response: See response to question 1.1. The website now allows for online submission of FOIA requests, which may include names, residential addresses, email addresses, and personal telephone numbers, as well as any other personal information that FOIA requesters enter into an open field to describe their requests.

1.6 Why is the information being collected, *e.g.*, what are the information system's purposes, intended uses, and/or functions: See response to question 1.1. Information from FOIA requesters is being temporarily collected to allow for submission of FOIA requests online. This will simplify the process for requesting records under the Freedom of Information Act.

1.7 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): Assigned by federal government
☐ 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: Older decisions published on the website may include copies of the wet signatures of former Commissioners and ALJs.
☐ 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)
☒ E-mail address(es): Assigned by federal government
☐ 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 non-OSHRC personnel or business customers, including (1) parties, attorneys, and/or representatives in OSHRC cases; (2) employees and other personnel who testify or are discussed in those cases; (3) E-Alert subscribers; and (4) FOIA requesters who submit requests through the website:

☐ Not applicable
☒ Individual's name:
☐ Other name(s) used, *i.e.*, maiden name, *etc*.
☐ OSHRC badge number (employee ID)
☐ SSN
☐ Race/Ethnicity
☒ Gender: Only to the extent this is evident from how an ALJ or Commission decision is written.
☐ 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: Only from FOIA requesters.
☐ Home address history
☒ Home telephone number(s): Only from FOIA requesters.
☒ Personal cell phone number(s): Only from FOIA requesters.
☒ Personal fax number(s): Only from FOIA requesters.
☒ Personal e-mail address(es): Only from E-Alert subscribers and FOIA requesters.
☐ 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: Only from parties, attorneys, and/or representatives in OSHRC cases.
☒ Other information:

The personal home and email addresses, and the home phone, personal cell phone, and personal fax numbers, can only be accessed and viewed by OSHRC system administrators. Business email

addresses, phone numbers, fax, numbers, and places of business may also be included in documents posted on the e-FOIA Reading Room.

Given the nature of the agency's adjudicative proceedings, various types of personal information could be included in a case record and in ALJ and Commission decisions. However, sensitive information is redacted before posting on the website, pursuant to OSHRC's redaction policy.

Finally, the online FOIA request form includes an open field for describing the request, which could result in any type of information—personal or otherwise—being submitted online by the requester. This information, however, is not accessible to the public.

"Non-personal" information obtained from FCC sources:

☒ Not applicable, Economic
☐ Data, Engineering scientific
☐ Data, Accounting/financial
☐ Data, Legal/regulatory/policy
☐ Data, Other information:

Miscellaneous Business, Technology, or Other Information:

☒ Not applicable
☐ Not publicly available business or technology data, *i.e.*, trade or propriety information
☐ Other information, please specify:

1.8 What are the sources for the 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:

1.9 Does this information system have any links to other information systems or databases? No. OSHRC's e-filing system can be accessed from the website by clicking a hyperlink, but the two components of the information system do not share or transfer data, or otherwise obtain data from one another.

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 skip to **Question 1.12**.

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

- ☐ Not applicable or none
- ☐ 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):
- ☐ 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:

Miscellaneous Business Information:

☐ Not applicable
☐ Not publicly available business data, i.e., trade or propriety information
☐ Other information:

"Non-personal" information:

☐ Not applicable Economic
☐ Data, Engineering/scientific
☐ Data, Accounting/financial
☐ Data, Legal/regulatory/policy
☐ Data
☐ Other information data provided

1.11 What are the sources for the information from the other information system (or database) that you are 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:

1.12 Will the information system derive new information or create previously unavailable information through aggregation or consolidation from the information that will now be collected, including

(where applicable) information that is being shared or transferred from another information system?

☐ Yes
☒ No

1.13 Can the information, whether it is: (a) in the information system; (b) in a linked information system; and/or (c) transferred from another system, be retrieved by a name or a "unique identifier" linked to an individual, *e.g.*, SSN, name, home telephone number, fingerprint, voice print, *etc*.?

☒ Yes
☐ No

OSHRC system administrators can search by the name of an E-Alert subscriber to obtain the email address provided by the subscriber. OSHRC system administrators can also search by the name or address for information submitted by FOIA requesters.

1.14 Will the new information include personal information about individuals, *e.g.*, personally identifiable information (PII), which is to be included in the individual's records or to be used to make a determination about an individual?

☒ Yes
☐ No

If the information system contains information about individuals, please answer **Question 1.15**; but if the information system does not contain information about individuals, please skip to **Question 1.16**.

1.15 What is the potential impact or "security risk" 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, inconvenience, or unfairness to the individual.

Please explain your response:

E-Alerts subscribers provide only a name and an email address, and this information may be accessed only by OSHRC system administrators. FOIA requesters using the online request form provide names, residential addresses, email addresses, and telephone numbers (either personal or business), as well as any other personal information that they enter into an open field to describe their requests. This information, however, is automatically deleted from the website's server after 120 days. Finally, with respect to documents—including ALJ and Commission decisions, as well as certain documents from case records—posted on the website, the most sensitive information is redacted pursuant to OSHRC's redaction policy.

1.16 Is this impact level consistent with the guidelines as determined by the FIPS 199 assessment?

☒ Yes
☐ No

If this information system component was compromised, it would result in a limited adverse effect. For example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

1.17 When was the information system last authorized or reauthorized pursuant to OMB Circular A-130? The agency reauthorized the information system on August 31, 2023.

1.18 Based on the information that you have provided thus far, choose one of the following:

☐ Based on the answers provided above, the information system (IT application or paper files) does not contain information about individuals nor does it have shared links with other information systems that may also contain information about individuals that could constitute a privacy issue.

A Privacy Impact Assessment (PIA) ***is not required*** *for this Information System.*

☒ Based on the answers provided above, the information system (IT application or paper files) does contain information about individuals, or it does have shared links with other information systems that may also contain information about individuals that could constitute a privacy issue.

A PIA ***is required*** *for this Information System.*