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 Local Area Network / Wide Area Network (LAN/WAN)

Date: 08/28/2019

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:**

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:**

This is a revision to a PIA that was completed on October 10, 2018. OSHRC has redefined the system covered by this PIA to be a component of a larger information system, "Occupational Safety and Health Review Commission Network and General Support System." The component of the information system covered by this PIA, previously named "General Support Systems (GSS)," has been renamed, "OSHRC Local Area Network / Wide Area Network (LAN/WAN)."

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

☒ Yes
Date: September 27, 2018. However, due to revisions made to the security categorization of this system, OSHRC is no longer relying on this PTA. It is therefore no longer attached to the PIA.

☐ 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: This information system component, now called OSHRC LAN/WAN, was previously referred to as GSS.

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 non-OSHRC personnel, including (1) parties, attorneys, and/or representatives in OSHRC cases; (2) employees and other personnel who testify or are discussed in those cases; and (3) Freedom of Information Act requesters:

☐ Not applicable
☒ Individual's name:
☐ Other name(s) used, *i.e.*, maiden name, *etc*.
☐ OSHRC badge number (employee ID)
☒ SSN: Commission procedural rules require parties to redact SSNs from exhibits or other materials filed with the agency, but sometimes SSNs are left unredacted.
☒ 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: Given the nature of adjudication, all possible types of personal information that could be included in a case record cannot be specified.

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? **No.**

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 1.10**.

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: Three SORNs cover different portions of the records stored on OSHRC's server: Emergency Contact Information, OSHRC-1; Payroll and Related Records, OSHRC-4; and Office of the General Counsel Records, OSHRC-5.

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 each of the SORNs is unclassified.

2.2 What is the location of the information covered by this SORN? As to the information addressed by this PIA, the information covered by the SORNs identified above is located electronically on a server at: OSHRC, 1120 20th Street, NW, Ninth Floor, Washington, DC 20036-3457.

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

Emergency Contact Information, OSHRC-1: Current OSHRC personnel, including Commission members, employees, and contractors.

Payroll and Related Records, OSHRC-4: Current and former employees of OSHRC and Commission members.

Office of the General Counsel Records, OSHRC-5: Current and former OSHRC attorneys (including supervising attorneys), Commission members, and Administrative Law Judges (ALJs);

Freedom of Information Act requesters; and parties in cases that have been, or presently are, before OSHRC.

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

Emergency Contact Information, OSHRC-1: (1) The names, home telephone numbers and addresses, and office telephone numbers of OSHRC personnel; (2) the names of emergency contacts, and the contacts' home telephone numbers and addresses, and office telephone numbers; and (3) the relationships between OSHRC personnel and their designated emergency contacts.

Payroll and Related Records, OSHRC-4: (1) Direct deposit records that include the employee's name and signature, address, and telephone number; the type of depositor account selected for direct deposit, and the account and routing numbers; and a voided check; (2) tax records that include the employee's name and signature, social security number, marital status, and home address; the number of allowances for which the employee qualifies; and further information which may be required on state, county, or city withholding certificates; (3) employee retirement estimates that include the employee's name and social security number; (4) records maintained pursuant to the Family Medical Leave Act that include the employee's name, signature, and job description; identity of certain family members and, if a child, date of birth; and medical information pertinent to leave requests; and (5) records necessary for payroll processing by NFC, including those pertaining to time and attendance and leave records, that may include some or all of the information specified above, as well as additional information concerning deductions, salary and benefits.

Office of the General Counsel Records, OSHRC-5: (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; (3) the names and job titles of the Commissioners and ALJs; (4) the names of FOIA requesters, contact information, and information concerning the requests; and (5) the names of OSHRC employees and the cases assigned to them, as well as the employees' contact information.

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

Emergency Contact Information, OSHRC-1: 29 U.S.C. § 661(e); 44 U.S.C. § 3101.

Payroll and Related Records, OSHRC-4: 5 U.S.C. §§ 301, 5516, 5517, 5520; 26 U.S.C. §§ 6011, 6109; 29 U.S.C. § 661; 44 U.S.C. § 3101.

Office of the General Counsel Records, OSHRC-5: 5 U.S.C. § 301; 5 U.S.C. § 552; 29 U.S.C. § 661; 44 U.S.C. § 3101.

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

Emergency Contact Information, OSHRC-1: The purpose of this system is to maintain current information on OSHRC personnel to allow office managers or other pertinent agency personnel to provide notification about, and/or respond to, emergency conditions.

Payroll and Related Records, OSHRC-4: Records are used by OSHRC and NFC employees to

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

maintain adequate payroll information for OSHRC employees and Commission members.

Office of the General Counsel Records, OSHRC-5: This system of records is maintained to assist management in making decisions with respect to case processing activities; to assist OSHRC attorneys in organizing their work product; and to assist in other matters assigned to the Office of the General Counsel, such as processing 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 (all SORNs).
☒ Court or Adjudicative Body: Routine Use 1 (all SORNs).
☐ Committee communications:
☐ Compliance with welfare reform requirements:
☒ Congressional inquiries: Routine Use 9 (all SORNs).
☐ Contract services, grants, or cooperative agreements:
☒ Emergency response by medical personnel and law enforcement officials: Routine Use 14 (OSHRC-1 only).
☒ Employment, security clearances, licensing, contracts, grants, and other benefits by OSHRC: Routine Use 3 (all SORNs).
☒ 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 (all SORNs).
☐ OSHRC enforcement actions:
☒ Financial obligations under the Debt Collection Act: Routine Use 20 (OSHRC-4 only).
☒ Financial obligations required by the National Finance Center: Routine Uses 14, 15, 16, 17, and 18 (OSHRC-4 only).
☐ 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 (all SORNs).
☒ Labor relations: Routine Use 5 (all SORNs).
☒ Law enforcement and investigations: Routine Use 2 (all SORNs).
☐ National security and intelligence matters:
☒ Department of State, Department of Homeland Security, and other Federal agencies: Routine Use 7 (all SORNs).
☐ Program partners, *e.g.*, WMATA:
☒ Breach of Federal data: Routine Uses 11 and 13 (all SORNs).
☒ Others Routine Use disclosures not listed above:

OSHRC-4

- **Routine Uses 19:** To the Federal Retirement Thrift Investment Board to update Section 401K type records and benefits; to the Social Security Administration to establish social security records and benefits; to the Department of Labor, Office of Worker's Compensation to process compensation claims; to the Department of Defense to adjust military retirement; to health insurance carriers to process insurance claims; and to the Department of Veterans Affairs for the purpose of evaluating veteran's benefits to which the individual may be entitled.

- **Routine Use 21:** To other federal, state, local or foreign agencies conducting computer matching programs to help eliminate fraud and abuse and to detect unauthorized overpayments made to individuals. When disclosures are made as part of computer matching programs, OSHRC will comply with the Computer Matching and Privacy Protection Act of 1988, and the Computer Matching and Privacy Protections Amendments of 1990.

- **Routine Use 22:** To the Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services, the names, social security numbers, home addresses, dates of birth, dates of hire, quarterly earnings, employer identifying information, and state of hire of employees for the purpose of locating individuals to establish paternity, identifying sources of income, and for other child support enforcement actions as required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 42 U.S.C. § 653(n).
- **Routine Use 23:** To "consumer reporting agencies" as defined in the Fair Credit Reporting Act (15 U.S.C. § 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. § 3701(a)(3)) in accordance with 31 U.S.C. § 3711(e)(1)(F).

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 permitted only in OSHRC-4 and only to the extent that disclosure would comply with 31 U.S.C. § 3711(e)(1)(F).

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

The information covered by all three SORNs is stored in access-restricted shared folders on OSHRC's server. Access to the server's network requires valid credentials, which can be either username and password or Government issued PIV card. The server is housed at the Commission's National Office, which is accessible using either an office key or access card. In addition, use of an access card is necessary to enter the specific room within the office that contains the server. Only the access cards of certain authorized employees and contractors—those responsible for maintaining the server—permit entry.

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

Emergency Contact Information, OSHRC-1: Electronic records, included in a spreadsheet, can be retrieved by name, telephone number, or home address.

Payroll and Related Records, OSHRC-4: Electronic records are retrieved by name.

Office of the General Counsel Records, OSHRC-5: Electronic records are retrieved by case name, docket number, name of OSHRC attorney or supervising attorney, or by the names of other individuals, such as FOIA requesters.

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

Emergency Contact Information, OSHRC-1: Records are retained until the subject of the record no longer works at OSHRC, at which time the paper record is shredded and the electronic file containing the record is revised to omit the subject's name and information.

Payroll and Related Records, OSHRC-4: Records are retained and disposed of in accordance with NARA's General Records Schedule 2.4.

Office of the General Counsel Records, OSHRC-5: Records are maintained in accordance with General Records Schedules 4.2 and 5.1, or for as long as needed for business use.

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

Emergency Contact Information, OSHRC-1: Information in this system of records comes from OSHRC personnel.

Payroll and Related Records, OSHRC-4: Information in this system either comes from the individual to whom it applies or is derived from information compiled by OSHRC employees performing administrative duties.

Office of the General Counsel Records, OSHRC-5: 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.

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: OSHRC's information technology staff consists of both 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?

☒ OSHRC staff in this bureau/office
☒ OSHRC staff in other bureaus/offices
☒ Information system administrator/Information system developers
☐ 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)?

Access to the shared folders is limited to employees and contractors who require access to perform their work duties.

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: Access is restricted based on instructions received from the pertinent OSHRC office manager.
☐ 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:

☒ Information system managers:
☒ Information system administrators:
☒ Information system developers:
☒ OSHRC staff in this bureau/office:
☒ OSHRC staff in other bureaus/offices in OSHRC area offices:
☒ Contractors:
☐ Other Federal agencies:
☐ State and/or local agencies:
☐ Businesses, institutions, and other groups:
☐ International agencies:
☐ Individuals/general public:
☐ 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)?

Contractors who have access to this information—those who work in OSHRC's information technology office, as well as those who work in other offices and require access to information to perform their work duties—receive the same Privacy Act and security awareness training, when first hired and then annually thereafter, that OSHRC employees receive.

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 *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: Many of the documents stored on the shared drive were submitted by parties during the adjudicatory process. As noted above, however, these documents are not subject to the Data Quality guidelines.

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: File server hard drives with need-to-know permission settings based on requests of office managers or data owners.

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 some of the records are maintained by the system manager identified in the SORN. For example, paper copies of certain FOIA records are maintained by the Office of the General Counsel, and paper copies of most of the case records are maintained by the Office of the Executive Secretary.

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

If the LAN/WAN became dysfunctional, the inability to access the system would "cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary function." *See* FIPS Publication 199. OSHRC's various offices would have difficulty performing their intended functions, as most of the offices' work product is stored on OSHRC's server. The availability of some paper records would allow the performance of some tasks to continue—such as case and FOIA processing, for example—though in a much less efficient manner.

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 will be minimal, as the PII is not, for the most part, disclosed to individuals or entities outside of the agency, and the PII is used only to the extent necessary to perform work activities, such as case processing, responding to FOIA requests, and internal administrative tasks.

5.7 Do individuals have the right to the following?

They may decline to provide their PII?

☐ Yes
☒ No

Most of the PII covered by this PIA is from case records (e.g., hearing transcripts and exhibits). Admission of these records into evidence and their use 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 releasing such documents to the public under FOIA, the documents are reviewed and redacted in accordance with 5 U.S.C. § 552(b)(6) and the Commission's redaction policy. Other PII covered by this PIA, such as PII provided by a FOIA requester (typically to allow the agency to respond with requested records) 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): Most of the PII covered by this PIA is from case records (e.g., hearing transcripts and exhibits). Admission of these records into evidence and their use is generally not in the control of the PII's subject. Refusal to provide documents including PII could be subject to the Commission's subpoena procedures (29 C.F.R. § 2200.65). However, as noted, 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.

If individuals do not have the right to consent to the use of their information, please skip to **Question 5.10**. (The PII is used only for the purpose for which it is collected.)

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

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

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; (FOIA requesters)
☒ The information is collected from the individual by e-mail; (FOIA requesters)
☒ The information is collected from the individual by completing an OSHRC form, license, and/or other document; (FOIA requesters—form is typically emailed upon completion)
☒ The information is collected from the individual by regular mail; and/or (FOIA requesters)
☒ The information concerning individuals is collected by other methods.

Please explain your response: Case records are typically downloaded from the Commission's e-filing/case management system and stored, for work purposes, in an access-restricted shared folder. Other documents, particularly those covered by OSHRC-1 and OSHRC-4, include information provided by new hires to the Commission's Human Resources Specialist.

FOIA requesters may provide their requests and contact information via email, regular mail, or fax.

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: Information is not submitted by individuals directly into this system. Privacy Notices are provided, however, when the documents are originally submitted (through the Commission's e-filing system, for example—see the PIA for that information system component).

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

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 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 this information system component, the pertinent SORNs, as well as this PIA, are reviewed on an annual basis. Finally, security awareness training and Privacy Act training are provided annually to 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**.

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: Some case record documents containing sensitive PII are maintained in their unredacted forms in shared access-restricted folders. Given the wide range of PII types that could be included in a case record, as well as the PII contained in emergency response records and any payroll records that may be maintained on the local server, the potential exists for moderate harm, embarrassment, inconvenience, or unfairness to the individual.

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? The aggregate security categorization for this information system component is moderate.

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? The agency is in the process of reauthorizing the information system, Occupational Safety and Health Review Commission Network and General Support System.

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:

As part of the reauthorization package for the Occupational Safety and Health Review Commission Network and General Support System, this information system requires a system security and privacy plan, and an assessment of security and privacy controls.

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/username/PIV requirements—protects the information from unintended disclosure.

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 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. Only information provided by FOIA requesters concerns the general public and that information is not solicited.

☐ 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:** (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 § 2400.5 (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 SORNs 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**: (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. Case records containing PII are stored in shared folders on OSHRC's server.	1. Shared folders are access-restricted to those employees who require access to perform their work duties. 2. Commission procedural rules (29 C.F.R. § 2200.8(c)(6), (d)(5)) minimize the amount of PII in documents that are admitted into evidence. 3. The Commission's FOIA and redaction procedures limit the amount of PII that is disclosed to the public when documents are requested or posted on oshrc.gov (see PIA for that information system component).
b. FOIA requester records containing PII are stored in shared folders on OSHRC's server.	1. Shared folders are access-restricted to those employees who require access to perform their work duties. 2. The Commission's FOIA and redaction procedures limit the amount of PII that is disclosed to the public when documents are requested or posted on oshrc.gov (see PIA for that information system component).
c. An emergency contact list containing PII is stored in a shared folder on OSHRC's server.	1. Shared folders are access-restricted to the system manager and office managers. 2. The information is maintained only as to current employees and contractors—the electronic file is revised to omit an individual's name and information once that individual no longer works for OSHRC.
d. Some documents covered by OSHRC-4 are stored in a shared folder on OSHRC's server.	1. Shared folders are access-restricted to those employees who require access to perform their work duties. 2. The documents are disposed of in accordance with the applicable General Records Schedule.

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: