

Occupational Safety and Health Review Commission



Privacy Impact Assessment (PIA)

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

Component: Americaneagle.com

Date: 08/14/2019

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:** November 2017

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, conducted on August 5, 2019, the SAOP and CIO have determined that a Privacy Impact Analysis is warranted.

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

- Yes
Date: August 5, 2019
- 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 addressed in a revision to the following SORN: [Database of Commission and ALJ Decisions, and Other Case-Related Documents, on OSHRC Website, OSHRC-8.](#)**

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? **The information is located on a web server at [Americaneagle.com](#), 2600 South River Road, DES Plaines, IL 60018.**
- 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 OSHRC’s website.

- 2.4 What are the categories of records¹ 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

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

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. Finally, this system includes a separate database that contains the names and email addresses of those individuals who subscribe to E-Alerts.

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.

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.

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.**
- 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.

- **Routine Use 15:** To Americaneagle.com to make certain that decisions published on OSHRC's website are current.

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 on a web server located at Americaneagle.com. OSHRC requests updates for its website through a secure portal which in turn updates a queue for posting by Americaneagle.com. Americaneagle.com secures information on the web server in accordance with federal standards. Access to the names and email addresses of those who subscribe to E-Alerts is limited to system administrators.

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

Records are listed on OSHRC's website by case name, docket number, and date, and can also be retrieved by using the search engine on the website's homepage to conduct a simplified Boolean search. Records are also retrievable by the names and email addresses of those who subscribe to E-Alerts.

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 N1455-11-003.

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 case records that are developed during adjudicative proceedings 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—names and email addresses—also comes from individuals who subscribe to E-Alerts.

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
- American Eagle (website)
- MicroPact (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
- 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)?

Americaneagle.com operates oshrc.gov, a public website. The public, therefore, has access to all information posted on the website. However, access to the names and email addresses of those who subscribe to E-Alerts is limited to system administrators, 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: *Information posted on oshrc.gov is available to the public, but the names and email addresses of E-Alerts subscribers is limited to 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 system administrators have access to the names and email addresses of E-Alerts subscribers. 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 a system administrator, that individual would 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 Understanding (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: 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, however, 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 on a web server located at Americaneagle.com.

- 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 Executive Secretary's office. 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](#).

- 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.

- 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; and (2) the E-Alerts subscribers' names and email addresses do not constitute particularly sensitive PII, this information is provided voluntarily, and it may be accessed by only system administrators (unless disclosed pursuant to a routine use).**

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—names and email addresses—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?

As to E-Alerts subscribers, names and email addresses must be provided to allow subscribers to receive updates. Individuals may opt not to sign up for the service.

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.

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

(Choose all the apply)

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

Please explain your response: Records are stored on a web server located at Americaneagle.com. OSHRC requests updates for its website through a secure portal which in turn updates a queue for posting by Americaneagle.com. Americaneagle.com secures information on the web server in accordance with federal standards. Before any documents are provided to Americaneagle.com, OSHRC's privacy office reviews the documents and redacts PII in accordance with its redaction policy.

As to the names and email addresses of E-Alerts subscribers, subscribers enter that information into textboxes on oshrc.gov. Once entered, the names and email addresses may be accessed only by system administrators.

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: Only names and email addresses, through the E-Alerts subscription process, is submitted through the website. A link to the privacy policy for oshrc.gov is at the bottom of the webpage.
- A Privacy Notice is printed at the end of the OSHRC form(s), license(s), and/or other Commission document(s): HRM collects information directly from OSHRC employees when they submit their bi-weekly payroll and leave data.
- The OSHRC Intranet site displays a Privacy Notice:
- The collection or input mechanism uses another method to provide individuals with the Privacy Notice:
- No Privacy Notice is provided:

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

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

Not applicable, as information will not be collected in this way.

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 system administrators will have access to names and email addresses submitted through the E-Alerts subscription process.

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, 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 this information system component, a PTA was conducted, which in turn necessitated the current PIA. Also, a revised SORN consistent with this PIA was issued in December 2018: [Database of Commission and ALJ Decisions, and Other Case-Related Documents, on OSHRC Website, OSHRC-8](#). Finally, security awareness training, as well as privacy training, is 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. (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 as part of the E-Alerts subscription process 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 not 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 does not constitute “information collection” under 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 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. Some case records containing PII are available to the public on the website's e-FOIA Reading Room.	1. Commission 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 limits the eliminate 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 system administrators.

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: Americaneagle.com

Date: 08/13/2019

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 Status:

1.1 Status of the Information System:

- New information system—**Implementation date:**
- Revised or upgraded information system—**Revision or upgrade date:** November 2017

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:

Through OSHRC's website, 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 system maintains a listing of the names of individuals who subscribe to this service and their email addresses. A new PTA, therefore, is being conducted.

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 collected from E-Alert subscribers was addressed in a revision to the following SORN: *Database of Commission and ALJ Decisions, and Other Case-Related Documents, on OSHRC Website, OSHRC-8 (Dec. 4, 2018).*

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. Names and email addresses will now

be collected to allow subscribers to receive E-Alerts.

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. Names and email addresses will now be collected to allow subscribers to receive E-Alerts.

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): **Government email**
- 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)
- E-mail address(es): **Government email**
- 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; and (3) E-Alert subscribers:

- 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 that gender 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
- Home address history
- Home telephone number(s)
- Personal cell phone number(s):
- Personal fax number(s)
- Personal e-mail address(es): Only from E-Alert subscribers.
- 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 addresses can only be accessed and viewed by IT personnel. Business email addresses, phone numbers, fax, numbers, and places of business may also be included in documents posted on the e-FOIA Reading Room.

Also, 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, the most sensitive information is redacted before posting on the website, pursuant to OSHRC's redaction policy.

“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

IT personnel can search by name of E-Alert subscriber to obtain the email address provided by the subscriber.

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:

With respect to E-Alerts, the subscriber provides only a name and an email address, and this information may be accessed only by IT personnel. 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? **This system is in the process of being reauthorized.**

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.