Office of Government Ethics

Privacy Impact Assessment for the Employee Administrative Records System (EARS)

May 2020

Compliance Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
Employee Administrative Records System

Provide electronic copies of the signed PIA to OGE's Chief Information Security Officer and Privacy Officer.

Name of Project/System: Employee Administrative Records System (EARS)
Office: Compliance Division

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Kaneisha Cunningham
Administrative Officer
Administrative Operations Branch
ktcunnin@oge.gov
202-482-9 228

2) Who is the system owner?

Compliance Division
Dale A. Christopher
Deputy Director for Compliance
dachrist@oge.gov
202-482-9224

3) Who is the system manager for this system or application?

Kaneisha Cunningham
Administrative Officer
Administrative Operations Branch
ktcunnin@oge.gov
202-482-9 228

4) Who is the Chief Information Security Officer who reviewed this document?

Ty Cooper
Chief Information Officer
jtcooper@oge.gov
(202) 482-9226

5) Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy
Chief, Legal, External Affairs and Performance Branch
diana.veilleux@oge.gov
(202) 482-9203

6) Who is the Reviewing Official?

Ty Cooper
Chief Information Officer
jtcooper@oge.gov
(202) 482-9226

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

The system serves as OGE's Emergency Notification System and administrative property management tool. It contains information on agency property assigned to particular OGE employees (such as a purchase card or a PIV card). It also contains emergency contact information about OGE employees.

Each employee has a single record that contains self-provided emergency contact information, as well as information added by the Administrative Officer about OGE-issued property. The system can generate a Microsoft Outlook email to communicate with employee government email accounts and personal email accounts as needed for emergency communications.

a. Is this information identifiable to the individual?

Yes.

b. Is the information about individual members of the public?

No.

c. Is the information about employees?

Yes.

2) What is the purpose of the system/application?

EARS allows OGE to track property assigned to its employees. It allows the Administrative Operations Branch to maintain and issue new property and facilitate exit clearance for departing employees. It also allows OGE to maintain emergency contact information for its employees and use provided contact information to send emergency

agency communications. Employees can access their own information to ensure that it is up-to-date.

3) What legal authority authorizes the purchase or development of this system/application?

The Ethics in Government Act of 1978, as amended, establishes OGE and authorizes the Director to provide overall direction of executive branch policies related to preventing conflicts of interest on the part of officers and employees of any executive agency. See 5 U.S.C. app. §§ 401-402. The development of this application is necessary for OGE to efficiently administer the necessary functions of managing its property and maintaining alternate means of contacting its employees in case of emergency.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

OGE employees.

2) What are the sources of the information in the system?

The emergency contact information is provided by the individuals themselves. The remainder of the information (not PII) is provided by the Administrative Officer from her knowledge of agency operations and incident to her responsibilities to issue, track, and collect agency property as part of OGE's administrative business processes.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The PII in the system (the emergency contact information) is obtained directly from the individual.

b. What federal agencies provide data for use in the system?

The General Services Administration (GSA) provides information regarding government purchase cards. The Administrative Officer also obtains information regarding PIV cards by logging into a GSA-maintained database called USAccess and printing out reports.

c. What State and local agencies are providing data for use in the system?

N/A.

d. From what other third party sources will data be collected?

N/A.

e. What information will be collected from the employee and the public?

The employee is asked to provide a personal telephone number, a personal email address, the name of an emergency contact person, and a telephone number for the emergency contact person.

3) Accuracy, Timeliness, Reliability, and Completeness

a. How will data collected from sources other than OGE records be verified for accuracy?

OGE employees are regularly reminded to check their emergency contact information and update it if necessary. The other information in the system is maintained by the Administrative Officer, who will verify it for accuracy in the course of agency operations (i.e. when government property is assigned/issued to an OGE employee or surrendered by the employee).

b. How will data be checked for completeness?

OGE employees are regularly reminded to check their emergency contact information and update it if necessary. The other information in the system is maintained by the Administrative Officer, who will check it for completeness in the course of agency operations (i.e. when government property is assigned/issued to an OGE employee or surrendered by the employee).

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

The data is current. OGE employees are regularly reminded to check their emergency contact information and update it if necessary. The other information in the system is maintained by the Administrative Officer, who will update it as necessary (i.e. when government property is assigned/issued to an OGE employee or surrendered by the employee).

d. Are the data elements described in detail and documented?

No. However, the data elements are simple and self-explanatory.

D. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No.

3) **Will the new data be placed in the individual's record?**

N/A.

4) **Can the system make determinations about employees/the public that would not be possible without the new data?**

N/A.

5) **How will the new data be verified for relevance and accuracy?**

N/A.

6) **If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?**

N/A.

7) **If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

N/A.

8) **How will the data be retrieved? Does a personal identifier retrieve the data?**

Data is retrieved by personal identifier and various reports (see below for description of reports).

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

EARS allows the Administrative Operations Branch to pull a list of property assigned to an employee. The Administrative Officer is able to access this information. The emergency contact information can also be provided in a list format to those who have been granted access through the AARF process, either because they have an

ongoing need to know based upon their work responsibilities (i.e. supervisors) or because they have been granted limited access for a specific, business-related purpose. Authorized individuals can also use the system to create a Microsoft Outlook email to communicate with employee government email accounts and personal email accounts as needed for emergency communications. To ensure privacy of the data, personal email addresses will be placed in the Blind copy address box.

10) What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?

Individuals do not have any opportunity to decline to provide the information or to consent to particular uses of the information. The information is necessary for the purposes outlined above and therefore, providing the information is mandatory and the uses are required.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A.

2) Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

Yes. The emergency contact information should be destroyed when superseded or obsolete, or upon separation or transfer of the employee (see General Records Schedule 5.3, Item 020). The administrative tracking files should be destroyed when superseded or when no longer needed for business use (see General Records Schedule 5.1, Item 010).

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Timely destruction of federal records is the responsibility of the Records Officer. The reports are temporary and will be destroyed when they are no longer needed by the agency. Emails generated by the system are subject to a 90-day auto delete policy.

4) Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

The use of the application should not have any measurable impact on public or employee privacy. There is no information in the application regarding the public. Employee information is used solely for official government business and protected with appropriate administrative and technical safeguards.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Individuals can be identified by name and address.

7) What kinds of information are collected as a function of the monitoring of individuals?

Information regarding home addresses and telephone numbers, as well as identification numbers associated with government property assigned to the employees (such as PIV cards and purchase cards).

8) What controls will be used to prevent unauthorized monitoring?

Each record will feature controlled access sections. Technical controls are in place to enforce role-based access to information. The Administrative Officer and other authorized OGE employees will have access to the property data only. Division Heads and Branch Chiefs will be granted access through the AARF process (see section F.2 below) to the emergency contact information, as required by OGE's Continuity Of Operations Plan (COOP). In addition, each employee will have access to all of their own data. Except as described above, employees cannot see other employees' data. Authorized users have been advised that agency policy prohibits them from unauthorized browsing of data or other misuse and have been instructed not to engage in such activities.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

OGE/INTERNAL-5, Employee Locator and Emergency Notification Records.

10) If the system is being modified, will the Privacy Act system of records notice (SORN) require amendment or revision? Explain.

The system of records notice does not require amendment or revision. Although the Privacy Act protected information in this system of records is nominally being kept in a different internal application than before, the two applications are the same in all relevant respects for the purposes of the SORN.

EARS will continue to display a current Privacy Act statement referencing OGE/INTERNAL-5 to OGE staff when they add or change their emergency contact information, as the prior Emergency Notification System did.

F. ACCESS TO DATA:

1) Who will have access to the data in the system?

The Administrative Officer and several other authorized OGE employees will have access to all the data in the application. Division Heads and Branch Chiefs will have access to the emergency contact information on their employees, as required by OGE's Continuity Of Operations Plan. In addition, each employee will have access to their own data. To ensure privacy of the data, personal email addresses will be placed in the blind copy address box if an employee is sent an emergency communication via email.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to OGE applications is governed by the Account Access Request Form (AARF) process, which authorizes the Information Technology Division (ITD) to create, modify, and disable network accounts, including providing access to OGE applications. AARF requests must be signed by the employee, their supervisor, and the Chief Information Officer before a request is approved to be implemented by ITD staff. AARF requests may be ongoing in nature, as with supervisors who have access to contact information about their employees, or temporarily granted for a specific, limited purpose.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Each record will feature controlled access sections. The Administrative Officer and other authorized OGE employees will have access to the property data only. Division Heads and Branch Chiefs will be granted access through the AARF process to the emergency contact information, as required by OGE's Continuity Of Operations Plan. In addition, each employee will have access to all of their own data. Except as described above, employees will not see other employees' data.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Technical controls are in place to enforce role-based access to information. In addition, authorized users have been advised that agency policy prohibits them from unauthorized browsing of data or other misuse and have been instructed not to engage in such activities.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

No contractors were involved with the design, development, or maintenance of the system.

6) Do other systems share data or have access to the data in the system? If yes, explain.

OGE Authorized users can create an email in Microsoft outlook from the system, to conduct emergency contact communications. Data is only sent when an action is taken by an authorized user, and data is not shared to or from any other applications at any other time.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Authorized users are responsible for using the interface according to agency policy. Use of the system does not impact the privacy rights of the public.

8) Will other agencies share data or have access to the data in this system (Federal, State, or Local)?

No.

9) How will the data be used by the other agency?

N/A.

10) Who is responsible for assuring proper use of the data?

Each authorized user is responsible for assuring proper use of the data.

See Attached Approval Page

The Following Officials Have Approved the
PIA for the Employee Administrative Records System:

1) **System Manager**

Initials: KC Date: 4/28/20

Name: Kaneisha Cunningham
Title: Administrative Officer

2) **System Owner**

Initials: DC Date: 4/28/20

Name: Dale A. Christopher
Title: Deputy Director for Compliance

3) **Chief Information Officer**

Initials: TC Date: 4/28/20

Name: Ty Cooper
Title: Chief Information Officer

4) **Senior Agency Official for Privacy**

Initials: DJV Date: 5/1/20

Name: Diana Veilleux
Title: Chief, Legal, External Affairs and Performance Branch
and Senior Agency Official for Privacy