Office of Government Ethics

Privacy Impact Assessment for OGE's Emergency Contact System

March 2025

Information Technology Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for OGE's
Emergency Contact System

Name of Project/System: Emergency Contact System

Office: Information Technology Division

I. EXECUTIVE SUMMARY

OGE's Emergency Contact System provides means for OGE leadership to contact employees outside of OGE's Microsoft 365 environment (i.e. on employees' personal accounts or devices). There are two elements of this system.

The first element is a web-based application called the "Emergency Notification System." It was developed in-house and is hosted on OGE's internal app portal. Participation in this application is mandatory for OGE employees. It functions as part of OGE's Continuity of Operations Plan (COOP).

Once implemented, the second element is a third-party web-based application called Constant Contact. Constant Contact is a digital marketing platform that helps businesses create and send email and SMS campaigns. Participation in the OGE Constant Contact initiative is voluntary. Employees may opt in and provide personal contact information if they wish to participate. Employees who choose to opt in should review Constant Contact's Privacy Notice as well as this PIA.

II. CONTACT INFORMATION

A. Who is the person completing this document?

Jennifer Matis
Privacy Officer
jmatis@oge.gov
(202) 482-9216

B. Who is the system owner?

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

C. Who is the system manager for this system or application?

Zohair Baig
IT Specialist
Information Technology Division

mzbaig@oge.gov
(202) 482-9311

D. Who is the Chief Information Security Officer who reviewed this document?

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

E. 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

F. Who is the Reviewing Official?

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

III. SYSTEM APPLICATION/GENERAL INFORMATION

A. Does this system contain any information about individuals?

Yes, it contains emergency contact information for OGE employees, including an individual designated as an emergency contact, a personal phone number, and a personal email address.

1) Is this information identifiable to the individual?

Yes.

2) Is the information about individual members of the public?

No.

3) Is the information about employees?

Yes.

B. What is the purpose of the system/application?

It allows OGE to maintain emergency contact information for its employees.

C. 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. 13121-13122. The development of this application is necessary for OGE to efficiently administer the necessary function of maintaining alternate means of contacting its employees in case of emergency.

IV. DATA in the SYSTEM

A. What categories of individuals are covered in the system?

OGE employees.

B. What are the sources of the information in the system?

The emergency contact information is provided by the individuals themselves.

1) 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?

N/A.

2) What federal agencies provide data for use in the system?

N/A.

3) What State and local agencies are providing data for use in the system?

N/A.

4) From what other third party sources will data be collected?

N/A.

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

For the mandatory Emergency Notification System, 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. In order to opt in to the Constant Contact initiative, the employee is asked to voluntarily provide their name and personal email address and/or telephone number.

V. ACCURACY, TIMELINESS, RELIABILITY, AND COMPLETENESS

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

It is the responsibility of the employee to provide accurate and complete information for both elements of the system. OGE employees are regularly reminded to check their emergency contact information in the mandatory Emergency Notification System and update it if necessary. With regard to Constant Contact, it is the responsibility of the individual to opt out of the initiative once they leave OGE or no longer wish to participate, as well as to maintain the accuracy of the information.

B. How will data be checked for completeness?

It is the responsibility of the employee to provide accurate and complete information for both elements of the system.

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. Employees can access their own information to ensure that it is current. They are regularly reminded to check their emergency contact information in the mandatory Emergency Notification System and update it if necessary. With regard to Constant Contact, it is the responsibility of the individual to opt out of the initiative once they leave OGE or no longer wish to participate, as well as to maintain the accuracy of the information.

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

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

VI. ATTRIBUTES OF THE DATA

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

B. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

C. Will the new data be placed in the individual's record?

N/A.

D. Can the system make determinations about employees/the public that would not be possible without the new data?

N/A.

E. How will the new data be verified for relevance and accuracy?

N/A.

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

N/A.

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

N/A.

H. How will the data be retrieved? Does a personal identifier retrieve the data?

Data in the mandatory Emergency Notification System may be retrieved by personal identifier. The information submitted to Constant Contact is not retrieved by personal identifier; it is used only in list format.

I. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The information in the mandatory Emergency Notification System can be provided in a list format to those who have been granted access through the AARF process (see below), 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. The information submitted to Constant Contact can be provided in list format to OGE officials with an administrative account. Access to the administrative accounts will be very limited and granted through the AARF process described below.

J. 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)?

With regard to the mandatory Emergency Notification System, 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. Providing information to Constant Contact is fully voluntary.

VII. MAINTENANCE AND ADMINISTRATIVE CONTROLS

A. 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.

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

The information in both elements of the system is maintained and/or destroyed in accordance with applicable OGE records disposition schedules and General Records Schedules (GRS) that are approved by the National Archives and Records Administration (NARA). OGE staff are informed of their recordkeeping responsibilities through training and meetings. Any information that is scheduled for disposal is destroyed in accordance with applicable records schedules, OMB, NARA, and NIST requirements.

C. 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?

Federal records are managed according to their content in accordance with NARA approved disposition authorities.

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

No.

E. How does the use of this technology affect public/employee privacy?

The use of the system has a small but necessary impact on employee privacy. The privacy controls in place are proportionate to the privacy risks. There is no impact on the public.

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

No.

G. What kinds of information are collected as a function of the monitoring of individuals?

N/A.

H. What controls will be used to prevent unauthorized monitoring?

N/A. The system does not have the capability to monitor individuals.

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

The information in the mandatory Emergency Notification System is maintained pursuant to OGE/INTERNAL-5, Employee Locator and Emergency Notification

Records. The application displays a Privacy Act statement. The information submitted to Constant Contact is not covered by the Privacy Act.

J. 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.

VIII. ACCESS TO DATA

A. Who will have access to the data in the system?

In the mandatory Emergency Notification System, each record features different levels of access. Division Heads and Branch Chiefs will be granted access through the AARF process (see below) to the emergency contact information, as required by OGE's continuation of operations plan. In addition, each employee will have access to all of his or her 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.

The privacy controls for the Constant Contact application are described in their Privacy Notice.

B. 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 access to OGE applications. AARF requests must be signed by the employee, his/her supervisor, and the Chief Information Officer before a request is approved to be implemented by ITD staff.

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

See above.

D. 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.

E. 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.

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

No other systems share data or have access to the data in the system.

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

N/A.

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

No.

I. How will the data be used by the other agency?

N/A.

J. Who is responsible for assuring proper use of the data?

The system owner is responsible for assuring proper use of the data.

See Attached Approval Page

The following officials have approved the PIA for the Emergency Contact System:

1) System Owner

Electronic Signature: JAMES COOPER

Digitally signed by JAMES COOPER
Date: 2025.03.25 16:16:50 -04'00'

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

2) Chief Information & Cybersecurity Officer

Electronic Signature: JAMES COOPER

Digitally signed by JAMES COOPER
Date: 2025.03.25 16:17:20 -04'00'

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

3) Senior Agency Official for Privacy

Electronic Signature: DIANA VEILLEUX

Digitally signed by DIANA VEILLEUX
Date: 2025.03.25 13:22:52 -04'00'

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