Office of Government Ethics

OGE Vaccination Documentation and Information System
Privacy Impact Assessment

January 2022

Compliance Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
OGE Vaccination Documentation and Information System

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

Name of Project/System: OGE Vaccination Documentation and Information System
Office: Compliance Division

A. CONTACT INFORMATION:

1) Who is the person completing this document

Jennifer Matis
Privacy Officer
Legal, External Affairs and Performance Branch
Program Counsel Division
jmatis@oge.gov
202-482-9216

2) Who is the system owner

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

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

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

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

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

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, it contains information about current OGE employees (not contractors).

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?

The purpose of this application is to collect proof of vaccination status from employees pursuant to guidance issued by OMB/the Safer Federal Workforce Taskforce. Pursuant to Executive Order 14043, all federal employees must be vaccinated (subject to limited exceptions) and agencies must verify their vaccinated status. In addition, OGE is authorized to collect verification of vaccination status (including boosters) in order to implement the safety policies embodied in OGE's Workplace Safety Plan.

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

5 C.F.R. part 293 subpart E; Executive Orders 13991 and 14043; and OMB Memoranda M-21-15 and M-21-25.

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 information is collected directly from the employees.

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?

See above.

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

Visual proof of vaccination (photo or scan), type of vaccine administered, date(s) of administration, and the name of the health care professional(s) or clinic site(s) administering the vaccine(s). The information may be related to initial vaccine administration and/or boosters.

3) Accuracy, Timeliness, Reliability, and Completeness

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

Employees will be required to certify that the information is correct. OGE employees are advised that providing false information may result in disciplinary action and a violation of federal law.

b. How will data be checked for completeness?

Not applicable.

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

The information is intended to be historical and will not be out-of-date.

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?

No.

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

No.

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

The data will be retrieved by vaccination status, vaccination type, division, and name of the employee.

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

A pre-built "view" or report will allow the data to be retrieved in different ways, including by name of the requesting employee. These views will be accessed and used by the Deputy Director for Compliance and the Chief of Staff for the purpose of ensuring the agency's compliance with E.O. 14043, the OGE Workforce Safety Plan, and OMB and Safer Workforce Task Force guidance.

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 may not consent to particular uses. Individuals are required to verify their primary vaccine status. Individuals may decline to provide booster status. However, those who do so will be treated as "not fully up-to-date on their vaccines" for the purposes of implementing the Workplace Safety Plan.

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?**

Not applicable.

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 records are covered by GRS 2.7 Health and Safety Records.

Note: The National Archives and Records Administration (NARA) is in the process of updating the GRS 2.7 Health and Safety Records disposition authority to include health-related records generated because of COVID-19.

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?

The records are short-term temporary records. They are to be destroyed 1 year after employee separation or transfer.

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 application has no effect on the public's privacy. Although it collects new PII from employees that was not previously collected, it collects no more than is necessary and properly secures the information. The impact on employee privacy is justified by the need for the information.

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

No.

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

Not applicable.

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

Not applicable.

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

OPM/GOVT-10.

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

The system of records notices do not require revision at this time.

F. ACCESS TO DATA:

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

An individual will have access to their own information. Beyond that, only the system manager or OGE's Chief of Staff have access to the EMFS records. The system uses the most restrictive controls available for the software, which allows access only to the individuals who created the entry ("reader") and system administrators. The records cannot be released outside of the agency without the written permission of both the system manager and OGE's Chief of Staff.

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, his/her supervisor, and the Chief Information & Cybersecurity Officer before a request is approved to be implemented by ITD staff.

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

See above.

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

Authorized users have been advised that agency policy prohibits them from unauthorized browsing of data and have been instructed not to engage in such activities. The system uses the most restrictive controls available for the software. Users of the system cannot access records that they are not authorized to access, thus preventing unauthorized browsing.

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 application.

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

No.

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

Not applicable.

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?**

Not applicable.

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

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

The Following Officials Have Approved the PIA for RT1201:

1) **System Manager and System Owner**

DALE CHRISTOPHER
Digitally signed by DALE CHRISTOPHER
Date: 2022.01.27 14:51:21 -05'00'

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

2) **Chief Information & Cybersecurity Officer**

JAMES COOPER
Digitally signed by JAMES COOPER
Date: 2022.01.27 15:15:48 -05'00'

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

3) **Senior Agency Official for Privacy**

DIANA VEILLEUX
Digitally signed by DIANA VEILLEUX
Date: 2022.01.28 14:27:00 -05'00'

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