Office of Government Ethics

Vulnerability Disclosure Policy
Privacy Impact Assessment

January 2022

Information Technology Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
Vulnerability Disclosure Policy

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

Name of Project/System: Vulnerability Disclosure Policy
Office: Information Technology Division (ITD)

Executive Summary

In accordance with Department of Homeland Security (DHS) Binding Operational Directive (BOD) 20-01 and Office of Management and Budget (OMB) Memo M-20-32, OGE has created a Vulnerability Disclosure Policy (VDP) to give security researchers clear guidelines for conducting vulnerability discovery activities on OGE systems and to describe how to submit discovered vulnerabilities to the agency. In addition, OGE plans to develop an application to manage the process that OGE will use to receive, track, respond to, and resolve reported vulnerabilities. This PIA covers both the VDP policy and application.

A. CONTACT INFORMATION:

1) Who is the person completing this document?

McEvan Baum
Assistant Counsel
Legal, External Affairs and Performance Branch
Program Counsel Division
mbaum@oge.gov
202-482-9287

2) Who is the system owner?

Zohair Baig
Deputy Chief Information Officer for Web Operations
mzbaig@oge.gov
(202) 482-9311

3) Who is the system manager?

Michael Murphy
IT Specialist
mmurphy@oge.gov
202-482-9312

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 and
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?**

Potentially, depending on whether researchers voluntarily share their contact information with OGE upon submitting a report. No information about individuals is required to be submitted.

a. Is this information identifiable to the individual?

Only to the extent a researcher voluntarily provides a name.

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

Potentially.

c. Is the information about employees?

Potentially.

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

The purpose of the policy and related application is to encourage researchers to contact OGE to report potential vulnerabilities in OGE's website and the *Integrity* electronic filing system for public financial disclosures so that OGE can investigate and resolve them.

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

DHS BOD 20-01 and OMB Memo M-20-32 require federal agencies to: (a) develop and publish a Vulnerability Disclosure Policy (VDP) for internet accessible production systems; and (b) enable the receipt of unsolicited reports. The purpose of this project is to comply with those requirements.

C. DATA in the SYSTEM:

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

Anyone who submits a vulnerability report to security@oge.gov and chooses to provide contact information.

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

The information is collected directly from the individual(s) reporting a vulnerability.

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 information is collected directly from the individual(s) reporting a vulnerability.

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

None.

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

None.

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?

The policy requests that researchers provide a detailed technical description of the steps required to reproduce the vulnerability, including a description of any tools needed to identify or exploit the vulnerability. Additionally, individuals making a report may voluntarily provide their contact information and any preferred methods or times of day to communicate so that OGE may contact them to clarify the reported vulnerability information or other technical information.

3) Accuracy, Timeliness, Reliability, and Completeness

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

OGE will rely on the researchers to provide their own information accurately, if they choose to provide contact information. Information on vulnerabilities will be verified in accordance with the OGE Vulnerability Disclosure Plan.

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?

Any submitted reports will be promptly acted upon.

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

Not applicable.

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?

Not applicable.

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 application contains a searchable database. It is possible to search by the researcher's email. OGE determined that the records are not covered by the Privacy Act because they are not "about" an individual.

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

No reports are produced on individuals.

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 submit reports anonymously.

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 DAA-GRS-2013-0005-0010 item 040. The retention period is Temporary. Destroy 5 years after the project/activity transaction is completed or superseded, but longer retention is authorized if required for business use.

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 procedures for the disposition of the data at the end of the retention period is included in OGE's Managing Electronic Records Guidance and Policy documentation.

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 policy and related application have only a minimal effect on privacy. Providing information is voluntary and the information is not sensitive.

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?

The system does not have the capability to monitor individuals.

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

Not applicable. The records are not subject to the Privacy Act because they are not "about" an individual.

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

Not applicable.

F. ACCESS TO DATA:

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

ITD has strict controls over the application database and only ITD has access to this particular application. The vulnerability reports are sent to a restricted access email account.

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.

Only OGE employees within ITD will have access to any information associated with the vulnerability reports within the application.

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. In addition, users 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.

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 Vulnerability Disclosure Policy:

1) **System Manager**

Electronic Signature: MICHAEL MURPHY Digitally signed by MICHAEL MURPHY Date: 2022.01.27 16:46:09 -05'00'

Name: Michael Murphy
Title: IT Specialist

2) **System Owner**

Electronic Signature: MIRZA BAIG Digitally signed by MIRZA BAIG Date: 2022.01.27 16:42:45 -05'00'

Name: Zohair Baig
Title: Deputy Chief Information Officer for Web Operations

3) **Chief Information & Cybersecurity Officer**

Electronic Signature: JAMES COOPER Digitally signed by JAMES COOPER Date: 2022.01.28 10:38:13 -05'00'

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

4) **Senior Agency Official for Privacy**

Electronic Signature: DIANA VEILLEUX Digitally signed by DIANA VEILLEUX Date: 2022.01.28 14:09:57 -05'00'

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