Office of Government Ethics

Box Content Management Platform
Privacy Impact Assessment

March 2023

Information Technology Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for Box Content Management Platform

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

Name of Project/System: Box Content Management Platform
Office: Information Technology Division

Executive Summary

Box is a third-party cloud-based collaborative content management platform. OGE uses Box to share information with various audiences and collaborate with stakeholders, including agency ethics officials. In addition to the privacy controls utilized in OGE's implementation of Box, Box has its own security and privacy program that includes customer-managed encryption keys, classification-based security controls, and AI-powered data leak protection and threat detection. More information on Box's security program is available on its website here. The Box online privacy policy is available here.

This PIA covers OGE's practices regarding the use of Box for managing content that does not contain personally identifiable information (PII). It also describes specific uses of Box for managing content that does involve PII, along with any additional privacy and/or security restrictions on such uses. For any other use of Box (that is, any use involving PII not specifically described below), OGE users should submit a Privacy Threshold Analysis (PTA) prior to that use being implemented and be prepared to abide by any additional restrictions set by ITD and/or the privacy team.

A. CONTACT INFORMATION:

1) Who is the person completing this document

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

2) Who is the system owner:

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

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

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

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

Ty Cooper
Chief Information & Cybersecurity Officer
Information Technology Division
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
Program Counsel Division
Diana.veilleux@oge.gov
202-482-9203

6) Who is the Reviewing Official?

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

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, it potentially contains information about current or former OGE employees and contractors, employees and contractors of other federal agencies, elected officials, and members of the public. OGE uses the system in two ways.

Use No. 1: The first way OGE uses Box is to post information (one-way). The audience for this information may be the public, OGE employees and contractors, employees and contractors of other federal agencies, or Congressional staffers. The information posted in this manner includes manuals or administrative information regarding the use of Integrity, ITD software for troubleshooting OGE laptops outside the network, and information about agency network status. Information posted to Box pursuant to Use No.1 should not contain PII except for the following:

- Public posting of the President's and Vice President's financial disclosure report or Executive Schedule I and II financial disclosure reports.
- Information provided to Congressional staffers appropriate for public release. "Appropriate for public release" means that although it may contain PII, it should not include any PII that OGE would not traditionally release to Congress via email or release to the public pursuant to the Freedom of Information Act.

The posting of any other type of PII requires an approved PTA before posting.

Use No. 2: The second way OGE uses Box is collaboratively to receive and/or maintain information from other federal agencies. The following collaborative uses are covered by this PIA pursuant to Use No. 2:

- Implementation of the Institute for Ethics in Government's (IEG) Accelerated Certification in Ethics (ACE) program. This use of Box includes a registration element, the submission of assignments, and assignment evaluations. The type of information collected and maintained includes non-sensitive PII such as the registrants' names, agencies, government email address, and grades received on ACE program assignments.
- Collection of Program Review work papers.

Note that the application by default collects IP address information from users accessing the website. OGE will not access or utilize that information, to the extent it is made available by Box.

The use of Box for any other collection of information requires an approved PTA.

a. Is this information identifiable to the individual?

Potentially, yes.

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

Potentially, yes.

c. Is the information about employees?

Potentially, yes.

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

OGE uses Box to share information with various audiences and collaborate with stakeholders, including agency ethics officials. See the Executive Summary above for more information.

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

The Ethics in Government Act of 1978, as amended, authorizes the Director of OGE 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. § 13122. Use of content management applications is an essential part of conducting agency business today. With regard to use of Box for training programs, OGE's responsibilities include supporting agency ethics officials through such training, advice, and counseling as the Director of OGE deems necessary. See 5 C.F.R. § 2638.108(a)(5).

4) What protections are in place to secure materials containing sensitive PII?

Note that under OGE's current uses for Box, the only sensitive PII that is authorized to be collected by or posted to OGE's Box account would be located within Program Review work papers (e.g. Confidential Financial Disclosure Reports). Box may not otherwise be used to transmit, collect, or maintain sensitive PII unless the user first submits a PTA and complies with any additional restrictions put into place.

OGE maintains tight control on its use of Box user accounts to ensure that all materials containing sensitive PII are properly secured. There is only one person, an OGE application developer, with access to most of the information on OGE's account, including the Program Review materials containing sensitive PII. The only other user accounts are assigned to *Integrity* and the IEG, neither of which collect nor post any sensitive PII. In addition, the application itself features a variety of protections, which are summarized in the Executive Summary above.

C. DATA in the SYSTEM:

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

- Current or former OGE employees and contractors
- Employees and contractors of other federal agencies
- Elected officials
- Members of the public

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

Information posted pursuant to Use No. 1 is provided by OGE employees and contractors from OGE records. It includes information originally collected from employees and contractors of other federal agencies, elected officials, and members of the public. The information collected pursuant to Use. No. 2 is provided by agency ethics officials.

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?

Potentially any executive branch agency may provide data.

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?

N/A.

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

See section B.1.

3) Accuracy, Timeliness, Reliability, and Completeness

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

Most of the information is from OGE records. For the remaining information, which is collected from agency ethics officials, it is the responsibility of the individual ethics official to ensure that they provide OGE with correct information.

b. How will data be checked for completeness?

Most of the information is not intended to be "complete," as the application is being used to transmit particular selections of information to various audiences. With regard to the information from agency ethics officials participating in the ACE program, it is the responsibility of the individual ethics official to ensure that they provide OGE with complete information.

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

The information from agency ethics officials participating in the ACE program is not intended to be kept current. Once the program is over, the need for the data is purely historical. With regard to the rest of the information, the content will be reviewed once a year as part of the annual website review process managed by the OGE web council. *Integrity* and IEG will each review their Box content and ITD will review the rest of the Box content.

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?**

The information related to the ACE Program and the financial disclosure reports are retrieved by personal identifier. No other information is retrieved by personal identifier.

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

N/A.

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.

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?**

Most of the records in the application are either duplicate copies or are only temporarily located in the application as a method to transmit them to more permanent locations. Training records maintained in the system are covered by the following existing records disposition authority: National Archives and Records Administration (NARA) disposition authority DAA-0522-2019-0007-003. The retention period is as follows: Cut-off at end of calendar year. Destroy 6 year(s) after cut-off.

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 agency Records Officer. The reports are temporary and will be destroyed in accordance with OGE NARA-approved records disposition schedules.

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 significant effect on public/employee privacy. The PII collected through or posted on the application would be collected and distributed through other means if not for the use of the application. The privacy and security controls on the application are at least as secure as the other means that would be used to collect and distribute the information through other means. Any impact on privacy has been minimized as much as possible and is justified by the need for the information.

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

The application does collect IP address information, however OGE will not be accessing that information.

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

N/A.

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

N/A.

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

The ACE training and performance information is collected and maintained pursuant to OPM/GOVT-2, Employee Performance File System Records. The ACE registration information is covered by OGE/INT-6, Online Registration for OGE-Hosted Meetings and Events. The financial disclosure reports are covered by OGE/GOVT-1, Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records. The other PII in the application is not retrieved by personal identifier; although it may originate from Privacy Act-protected records (e.g. confidential financial disclosure reports contained in Program Review work papers).

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

No Privacy Act system of records notice will require amendment or revision.

F. ACCESS TO DATA:

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

As discussed above, very few individuals have access to OGE's Box account. OGE has three accounts—one assigned to an OGE application developer, one assigned to an *Integrity* staffer, and one assigned to an IEG trainer.

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

Access to OGE applications and user accounts 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.

Users will only have access to the data they are authorized to access. The individuals managing OGE's box accounts can restrict access further within each accounts to ensure limited access.

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

Because administrative access is restricted to a very limited number of authorized individuals, there is no potential for 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.**

There is no direct interface with other systems.

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

N/A.

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 user is responsible for assuring proper use of the data.

See Attached Approval Page

The Following Officials Have Approved the PIA for Box Content Management Platform:

1) **System Manager**

   Initials: TC Date: 3/6/23

   Name: Ty Cooper
   Title: Chief Information & Cybersecurity Officer,
   Information Technology Division

2) **System Owner**

   Initials: TC Date: 3/6/23

   Name: Ty Cooper
   Title: Chief Information & Cybersecurity Officer,
   Information Technology Division

3) **Chief Information Officer**

   Initials: TC Date: 3/6/23

   Name: Ty Cooper
   Title: Chief Information & Cybersecurity Officer
   Information Technology Division

4) **Senior Agency Official for Privacy**

   Initials: DJV Date: 3/7/23

   Name: Diana Veilleux
   Title: Chief
   Legal, External Affairs and Performance Branch
   Program Counsel Division