

**Pension Benefit Guaranty Corporation (PBGC)
Privacy Impact Assessment (PIA)**



**Office of General Counsel (OGC) Government to
Government (OGCG2G)**

Integrity

06/07/2024

1 Privacy Point of Contact

Name	James Burns
Title	Information Owner
Phone	202-229-3525
Email	Burns.James@PBGC.gov

TIP!

This point of contact should be the person you want the Privacy Office to work with in completing this PIA. For some systems it might be the Information Owner (IO) or Information System Owner (ISO). Many business units identify this as the Information System Security Officer (ISSO). DO what makes sense for you!

2 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information is/will be handled:

- i. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
- ii. To determine risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system, and
- iii. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many types of information that can be used to


distinguish or trace an individual's identity, the term PII is necessarily broad.

TIP!

Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

2.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII?	In what system of records (SORN) is this information stored?	What is the Legal Authority for collection of this information?	Does this system share PII internally? <i>(Please detail in question 9)</i>
Integrity	Integrity is an electronic financial disclosure system created by the U.S. Office of Government Ethics (OGE). Integrity provides a secure, Web-based system through which individuals may file executive branch public financial disclosure reports.	Yes	<p>OGE/GOVT-1</p> <p>https://www.oge.gov/Web/oge.nsf/0/36AA5AF46B37641C852585B6005A1532/\$FILE/GOVT-1%20(Nov%202016).pdf</p>  <p>OGE GOVT-1 2019 Federal Register No1</p>	Stop Trading on Congressional Knowledge Act of 2012 (“STOCK Act”), Pub. L. No. 112-105, 125 Stat. 191, 298-99 (2012), (as amended); EIGA, 5 U.S.C. app. § 101 et seq as amended.	No

2.2 The System as a Whole

1. Please describe the purpose of the system, when considered as a whole, please include if this is an existing system (either an annual recertification update or a major change)

The Stop Trading on Congressional Knowledge Act of 2012 (STOCK Act) directed U.S. OGE to develop Integrity and mandated all federal agencies and applicable employees to use the system for electronic financial disclosure. Integrity is operated and owned by the U.S. Office of Government Ethics (OGE). OGE also owns the data within Integrity. PBGC employees are the users of the system. U.S. OGE issued an Authorization to Operate (ATO) for Integrity on 12/24/2014.

Integrity provides a secure, Web-based system through which individuals may file executive branch public financial disclosure reports. Integrity also makes it easy for ethics officials to assign, review, and manage the reports electronically.

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Low

3. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.); the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.); the notification given at time of collection from an individual regarding the Privacy Act and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

Integrity collects PII from individuals via electronic forms. Use of the system constitutes a user's consent to sharing their information with authorized users. By using the system, filers consent to the specific uses of their Personally Identifiable Information (PII). The system presents a standard information system use and consent banner at login. The system login page displays this message:

Notice:

WARNING: This is a U.S. Government computer system, use of which is subject to federal law. Unauthorized use of this system is prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986.

The system login page also includes a link to the full Privacy Act statements related to the system. The following is the Privacy Act Information from Integrity.gov:


<https://extapps2.oge.gov/integrity/help.nsf/docs/Privacy+Information>



Integrity Privacy
Information 2021060

4. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third-party provider, another government agency, etc.). If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy-applicable portions of that document.

PBGC does not fully inherit any privacy controls from OGE. No ISA is required because there is no dedicated connection. OGC signed a Memorandum of Agreement (MOA) in April 2015 with U.S. Office of Government Ethics (OGE) for Integrity. The MOA indicated that U.S OGE is responsible for the incident response (IR) on a PII data breach. If the data breach is first identified by PBGC, then PBGC should follow its agency IR plan and notify U.S OGE. The following is the attached MOA.



PBGC MOA.PDF

5. For the user roles in the system:

Role Name	# of Users	Approver	Access Level (Read, Write, etc.)	Recertification Date
APPS_OGE_Integrity_ActiveFiler	37	James Burns; Thom Verratti	Write (individual filing only)	User count as of June 7, 2024
APPS_OGE_Integrity_Reviewer	8	James Burns; Thom Verratti	Read/write (adjudications)	User count as of June 7, 2024
APPS_OGE_Integrity_Maintenance	2	James Burns; Thom Verratti	Read/write (user control only)	User count as of June 7, 2024
APPS_OGE_Integrity_DAO	2	James Burns; Thom Verratti	Read/write (user control only)	User count as of June 7, 2024

6. Does the System leverage the Enterprise Access Controls?

- Yes
- No

7. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

Physical Controls:

Integrity leverages U.S. OGE physical security controls employed to secure the PII in the system. These controls include security guards, key entry, and secured facility.

Technical Controls:

Integrity leverages U.S. OGE technical security controls employed to secure the PII in the system. These controls include password protection, configuration management, contingency planning, audit logging, firewalls, unique user identification names, encryption, intrusion detection systems, and vulnerability scanning.

PBGC is responsible for reviewing and approving PBGC user access requests and performing annual user account recertifications.

Administrative Security Controls:

Integrity fully leverages U.S. OGE incident response controls to secure the PII in the system. Awareness and Training, Incident Response, Personnel Security, Planning, and Security Assessment and Authorization (SA&A) controls are hybrid between OGC and the Environmental Protection Agency (EPA). For example, OGC conducts annual SA&A processes and reviews U.S. OGE's SA&A package on-site at least annually.

8. For the PII in the system, discuss the actual/intended uses of the PII; the steps taken to limit the PII collected to the minimum needed; and the reasons the PII is necessary and relevant.

Filers provide their reportable personal and financial disclosure information in accordance with the Ethics in Government Act of 1978 as amended.

Any individual who uses the system must provide minimal contact information such as agency, business address, telephone number, and official email address. Filers using the system provide their official position title and reportable personal financial information.

9. Discuss the data flows within the system (include sources of data for data flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

Filers log in to Integrity via Web browsers and complete the electronic U.S. OGE Form 278. The PBGC Reviewers then review the forms. PII remains within Integrity while data disclosure is controlled by U.S. OGE.

Integrity does not have any interconnections. OGC still signed a Memorandum of Agreement (MOA) in April 2015 with U.S. OGE for Integrity and is attached in *Appendix D: PBGC and OGE MOA for Integrity*.

10. Does the system leverage the commonly offered control for Accounting of Disclosures?

- Yes
- No

11. If your system collects, Social Security Numbers:

- a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of Social Security Numbers (SSN).

Integrity does not collect Social Security Numbers.

Enter description here.

- b. Under which authorized uses, as described in the “Reduction of Use of Social Security Numbers (SSN) in PBGC” policy document?
- c. If the answer to b., above, is “Compelling Business Need,” please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

Enter description here.

2.3 Privacy Office Review

Name of Reviewer	William Black WILLIAM Digitally signed by WILLIAM BLACK
Date Reviewed	7/2/2024 BLACK Date: 2024.07.23 08:13:14 -04'00'
Expiration Date	Twelve months from date of review by the Privacy Office
Result	<input checked="" type="checkbox"/> Approved without conditions <input type="checkbox"/> Approved with conditions (see below). <input type="checkbox"/> Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps.

Enter description here.

Discuss any conditions on Approval

Enter description here.