Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Integrity Privacy Impact Assessment (PIA)

Last Updated: 06/25/2026

1 Privacy Point of Contact

Name	Catherine Diamante
Title	Information System security and Privacy Officer (ISSPO)
Phone	202.229.6039
Email	Diamante.Catherine@pbgc.gov

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 *(please detail in question 13)*
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	OGE/GOVT-1	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. Office of Government Ethics, 89 Fed. Reg. 17470.	No

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole.

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 10/15/2024.

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. Is this a contractor system?

☒Yes
☐No

4. Is this a new or existing information system? If this is an existing information system, please describe the changes.

This is an existing system and there are currently no changes.

5. Does your system collect, process, or maintain any records that describe how any individual exercises their First Amendment rights?

   If so, please describe the information it collects and the purpose for the collection. Please describe whether: 1) an express legal authority authorizes the collection, 2) the collection is pertinent to and within scope of an authorized law enforcement activity, or 3) the individual(s) consents to the collection.

   (The First Amendment guarantees an individual's right to the exercise of their religious beliefs, their petitioning the government, their exercise of free speech, their right to peaceably assemble, and the freedom of the press.)

No, the system does not collect, process, or maintain any records that describe how any individual exercises their First Amendment rights.

6. For the PII in the system, discuss the actual/intended uses of the PII; procedures taken to limit the PII collected to the minimum needed; reasons the PII is necessary and relevant; and procedures taken to periodically review the accuracy, relevance, timeliness, and completeness of PII throughout the information life cycle.

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

Restricted fields are in place to limit PII collected and accessed to only the minimum necessary.
Any individual who uses the system must provide minimal contact information such as agency, personal contact information, business address, telephone number, and official email address. Filers using the system provide their official position title and reportable personal financial information.

The filer information so provided is used only for review by Government officials of the federal employee's agency and determining compliance with applicable federal conflict of interest laws and regulations.

7. Discuss how your system retrieves PII. Please describe the identifiers used to locate records within a system, such as name, identification number, date of birth, etc.

Filers provide and access their own information against their PBGC email address and Integrity login. Records are listed, retrieved, reviewed, and adjudicated by filer name, with filing year serving as the secondary key. Annually filed forms 278 are connected to the relevant PBGC employee.

8. Approximately how many individuals' PII is maintained in the system?

35 PBGC Filers

9. Is the submission of PII by individuals voluntary or mandatory? If the submission is voluntary, what is the outcome of an individual not submitting PII.

The submission of PII is mandatory.

10. 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 SSN?

Integrity does not collect Social Security Numbers.

b. Under which authorized uses, as described in the "Reduction of use of Social Security Numbers (SSN) in PBGC" policy document?

N/A

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.

N/A

11. 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: The system login page includes a link to the full Privacy Act statements related to the system.

12. 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 all privacy controls from OGE; however, OGE does provide several key privacy controls; specifically PT-02, PT-03, PT-04, PT-05(2), and PT-6, for Integrity . 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.

13. Is the PII shared with external (non-PBGC) organizations? If so, identify with whom the PII is shared and the purpose. 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 signed a Memorandum of Agreement (MOA) in April 2015 with U.S. OGE for Integrity.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
APPS_OGE_Integrity _ActiveFiler	34	James Burns; Thom Verratti	Write (individual filing only)	05/08/2026
APPS_OGEIntegrity _Reviewer	8	James Burns; Thom Verratti	Read/write (adjudication)	05/08/2026
APPS_OGE_Integrity _Maintenance	2	James Burns; Thom Verratti	Read/write (user control only)	05/08/2026
APPS_OGE_Integrity _DAEO	2	James Burns; Thom Verratti	Read/write (user control only)	05/08/2026

15. 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.
Physical security controls employed to secure the PII in the system include:

Physical Access Authorizations
Physical Access Control
Access Control for Transmission Mission
Access Control for Output Devices
Monitoring Physical Access
Access Records
Power Equipment and Power Cabling
Emergency Shutoff
Emergency Power
Emergency Lighting
Fire Protection
Temperature and Humidity Controls
Alternate Work Site
Location of information Components
Information Leakage

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
Technical Controls - Technical controls employed to secure the PII in the system include:
Account Management
Access Enforcement
Authenticator Management
Cryptographic Module Authentication
Cryptographic Protection
Separation of Duties

Least Privilege
Device Lock
Remote Access
Wireless Access
Information Sharing
Audit Events
Audit Review, Analysis, and Reporting
Time Stamps
Audit Record Retention
Media Storage
Media Sanitization
Consent
System of Record Notice
Privacy Notice
Public Key Infrastructure Certificates
Denial of Service Protection
Transmission Confidentiality and Integrity
Network Disconnect
Flaw Remediation
Protection of Information at Rest
Process Isolation
Malicious Code Protection
System Monitoring
Security Alerts, Advisories and Directives
Information Integrity
Spam Protection

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.
Administrative Controls - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system include:

- *Personnel Screening*
- *Information Requiring Special Protection Measures*
- *Access Agreements*
- *Authorization*

- *External Personnel Security*
- *Continuous Monitoring*
- *Incident Response Plan*
- *System Security and Privacy Plans*
- *Personnel Screening*
- *Annual Security, Privacy, and Records Management Refresher Training*
- *Role-Based Training*

16. Please discuss additional training for users, other than the PBGC mandatory annual training, for protecting information in the system.

N/A

17. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

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

☐ Yes
☒ No

19. Discuss the process in place for retention and destruction of PII. Cite the applicable

The OGE procedures for the disposition of data at the end of the retention period are in accordance with the National Archives and Records Administration General Records Schedule 2.8 Employee Ethics Records: These records are generally retained for a period of six years after filing, or for such other period of time as is provided for in that schedule for certain specified types of ethics records.
In cases where records are filed by, or with respect to, a nominee for an appointment requiring confirmation by the Senate when the nominee is not appointed and Presidential and Vice-Presidential candidates who are not elected, the records are generally destroyed one year after the date the individual ceased being under Senate consideration for appointment or is no longer a candidate for office.

However, if any records are needed in an ongoing investigation, they will be retained until no longer needed in the investigation. Destruction is by shredding or electronic deletion.

2.3 Privacy Office Review

Name of Reviewer	Loretta Dennison
Date Reviewed	June 25, 2026
Expiration Date	June 25, 2027
Result	☒ Approved without conditions ☐ Approved with conditions (see below). ☐ 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
