Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Veritone

Privacy Impact Assessment (PIA)

Last Updated: 08/27/2025

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.

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)*
Veritone Redact	Cloud service to which a media document (audio or video) can be copied and which gives a user the ability to redact the document (remove portions of the audio and/or video), apply exemptions to the redactions (label each redaction as to the exemption statute which applies), and copy this redacted version of the file back to the calling service. Used in our case by the Disclosure Access Portal (DAP) solution FOIAXpress.	Yes	PBGC-29: Freedom of Information Act and Privacy Act Request Records	5 U.S.C. § 552, The Freedom of information Act (FOIA) as amended, The Privacy Act of 1974, as amended, 5 U.S.C. §552a, and 29 CFR Part 4901-4902 as amended.	Yes

2.2 The System as a Whole

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

The Veritone Redact service (hosted by Veritone's aiWARE for Government cloud) provides review and redaction of audio and visual documents (i.e., sound files and video files).

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

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

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 a new information system

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.)

Veritone Redact may process video or audio files that describe how an individual (e.g., protest footage) exercises their First Amendment rights. It is not a system of record for that footage, and those inquiries should be referred to PACSS.

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.

Intended use of PII is to respond to Privacy Act or FOIA requests. The system creates copies of files before being redacted and only relevant files which may contain PII are uploaded to Veritone Redact. Veritone Redact allows the user to bring in one media file at a time for review and editing (the application of redactions and exemptions) and has the file and its edited version in its boundary for as long as the user needs to work on it. When the user is done, a copy of the newly edited (redacted) version of the media file is sent to the DAP (FOIAXpress). The user removes all originals and all edited copies of the file from Veritone Redact as the final step. No files are retained or kept in Veritone Redact after the user is done creating the edited version.

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.

Veritone Redact does not retrieve information by PII.

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

Only a very small fraction of FOIA or Privacy Act requesters will be getting responsive audio or video files which are processed through Veritone Redact – as of 2025, our estimate is that PBGC might release between zero (0) and five (5) such files each year.

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.

N/A. The PII is not being submitted by individuals.

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?

    Veritone Redact does not collect PII, including Social Security Numbers. However, files submitted for redaction may contain 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. Social Security Numbers might be included in a file, but they are not being used as a primary identifier.

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.

Veritone Redact only receives data from DAP. Please see the PIA for DAP.

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 inherit privacy controls from any external provider.

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.

The redacted copy of the file is sent back to FOIAXpress. See PIA for DAP.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
FOIA Administrator	2	James Burns	Full Access to All Role Permissions (other than configuration) (Read, Write, Delivery, Deletion)	3/28/2025

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Government Information Specialists	12	James Burns	Access to All Request Type Role Permissions and File Cabinet Drawer Permissions Only (Read, Write, Delivery & Deletion Capabilities)	3/28/2025
FOIA Appeals	6	James Burns	Access to the Appeals Adjudication Functions and File Cabinet Drawer Permissions (Read, Write, & Delivery Capabilities)	3/28/2025
FOIA Professional	1	James Burns	Limited Request Type Role Permissions (Read & Write Capabilities)	3/28/2025

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

Physical Controls - 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*
- *Visitor Control*
- *Access Records*
- *Power Equipment and Power Cabling*
- *Emergency Shutoff*
- *Emergency Power*
- *Emergency Lighting*
- *Fire Protection*
- *Temperature and Humidity Controls*
- *Delivery and Removal*
- *Alternate Work Site*
- *Location of information Components*
- *Information Leakage*

**Physical Controls are provided by both PBGC and the Cloud Service Provider (CSP)*

*Technical Controls** - Technical controls employed to secure the PII in the system include:*

- *Account Management*

- *Access Enforcement*
- *Authenticator Management*
- *Cryptographic Module Authentication*
- *Information Flow Enforcement*
- *Separation of Duties*
- *Least Privilege*
- *Unsuccessful Login Attempts*
- *Remote Access*
- *Wireless Access*
- *Audit Events*
- *Audit Review, Analysis, and Reporting*
- *Time Stamps*
- *Audit Record Retention*
- *Non-repudiation*
- *Session Audit*
- *Public Key Infrastructure Certificates*
- *Denial of Service*
- *Network Disconnect*
- *Session Authenticity*
- *Protection of Information at Rest*

***Technical Controls are provided by both PBGC and the CSP*

Administrative Controls - Administrative controls employed to secure the PII in the system include:

- *Periodic Security Audits*
- *Regular Monitoring of User's Activities*
- *Annual Security, Privacy, and Records Management Refresher Training*
- *Backups Secured Offsite*
- *Encryption of Backups containing sensitive data*
- *Role-Based Training*
- *Least Privilege Access*
- *Mandatory on-boarding training for security, privacy, and Records management personnel - All PBGC users are required to complete privacy training annually.*

These general principles (taken from the DAP) apply to any documents processed by Veritone Redact.

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

Disclosure Division users take periodic training on the FOIA and Privacy Act provided by the Department of Justice and Division leadership. These trainings include discussions and presentations and cover general handling and protecting of PII.

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 retention schedule(s).

Veritone Redact does not retain any documents or records. Documents processed by Veritone Redact are passed back to FOIAXpress (in the DAP) and are not held in the Veritone boundary.

2.3 Privacy Office Review

Name of Reviewer	Loretta Dennison
Date Reviewed	August 26, 2025
Expiration Date	August 26, 2026
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