Pension Benefit Guaranty Corporation

Information Technology Infrastructure and Operations Department (ITIOD)

PSIS Privacy Impact Assessment (PIA)

Last Updated: 08/06/2021

1 PRIVACY POINT OF CONTACT

Name	Tod Ware
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.6229
Email	Ware.Tod@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 9)*
eDelivery	eDelivery is an electronic solution hosted by DCSA. It provides PBGC's Information Technology Infrastructure Operations Department (ITIOD) with the ability to securely retrieve investigative files to process, adjudicate, and track the status of background investigation cases.	Yes	PBGC- 12 - Personnel Security Investigation Records	PBGC's authority to collect information is derived from: 29 U.S.C. 1302; 5 U.S.C. 3301; 44 U.S.C. 3101; Executive Order 10450; Executive Order 10577; Executive Order 12968; Executive Order 13467; Executive Order 13488; 5 CFR 5.2; 5 CFR 731, 732 and 736; 5 CFR 1400; OMB Circular No. A-130 Revised, Appendix III, 61 FR 6428; Federal Information Processing Standard 201; Homeland Security Presidential Directive 12	Yes

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).

PSIS is a background investigation and security clearance query application. This application is a case management system that enables ITIOD to update and query relevant information about employees' and contractors' background investigations and security clearances. PSIS uses the separate eDelivery system to securely retrieve investigative files to process, adjudicate, and track the status of PBGC background investigation cases.

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

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

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.

All investigative case details, including PII, shall be retained in a secure IT system or safe with restricted access. Some information, such as UPN and AD-ID, are pulled from other systems (General Services Administration (GSA) reports and Active Directory). The Defense Counterintelligence and Security Agency (DCSA) randomly mails hard copy documents & case files to PBGC Personnel Security, this information is scanned and uploaded into PSIS.

PSIS Information is collected from individuals, other Federal agencies, phones, websites, and from other information systems.

PII data is ingested from PSIS to Symantec DLP for Exact Data Matching. The ingested data includes federal and contractor personnel PII (first name, last name, SSN, and DOB). The data values are updated during the ingestion and only the hash values are stored in DLP. The DLP policies for PSIS were last updated on 7/21/2021.

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.

No privacy controls are inherited from any external providers. There is a valid MOU between PBGC and DCSA (Agreement Number: 796). Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies. In order to comply with the provisions of the Privacy Act, Personally Identifiable Information (PII) captured will be secured in compliance with the Federal Information Security Management Act (FISMA) and not subject to unauthorized distribution.

5. For the user roles in the system:

Role Name	Number of Users in that Role (AD)	Approver	Access Level (Read, Write, etc.)	Recertification Date
Adjudicator	3	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Admin Read Only	3	Manager/COR and PSIS Administrator	Read, Search	Annually
Administrator	12	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Federal Team Member	4	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Search	Annually
Manager Reviewer	0	Manager/COR and PSIS Administrator	Read, Write, Update, Search	Annually
Security Assistant	2	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Security Specialist	8	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually

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 - Entrance to PBGC HQ facilities employ armed guards and a PIV activated turnstile. Suites, to include the Network Operations Center (NOC), require a PIV for physical access. Physical security controls employed to secure the PII in the system include:*
  - *Security guards*
  - *Security Guards*
  - *Secured Facility*
  - *Key Entry*
  - *Identification Badges (PIV)*
  - *Locked Offices*
  - *Locked File Cabinets*
- *Technical Controls - All PBGC users are required to go through the PBGC GetIT Service Portal to request privileges to systems/applications. The granting of privileges is based on least privilege and separation of duties. Technical controls employed to secure the PII in the system include:*
  - *Password protection*
  - *Virtual Private Network (VPN)*
  - *Firewalls*
  - *Unique user identification names*
  - *Encryption*
  - *Intrusion Detection Systems (IDS)*
  - *Personal Identity Verification (PIV) card access*
  - *Public Key Infrastructure (PKI) Certificates*
- *Administrative Controls - All PBGC users are required to complete privacy training annually. 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*

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.

PII is retrieved from completed background investigations from DoD to support the suitability determination process of federal and contractor personnel. PII is then used to conduct background investigations of federal and contractor personnel.

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.

Currently, PSIS leverages the eDelivery interface as outlined in the PBGC and DCSA Memorandum of Understanding (MOU) to securely retrieve investigative files. The MOU is located in CSAM and was signed 07/09/2020.

eDelivery consists of three distinct aspects: the content, packaging, and delivery of investigative case material.

Content

The investigative content of the eDelivery investigative case material file will be identical to the investigative content of a mailed hard copy version of the investigative case material.

Packaging

eDelivery packages the contents of an investigative file in a 256-bit encrypted ZIP file, the Distributed Investigative File (DIF). The DIF serves as an electronic representation of the investigative file and provides both a graphic representation of a printed file and a data representation of certain documents.

Delivery

PBGC investigative case material will be transferred via a nightly batch transmission. The transmission will include a crosswalk manifest listing all cases included in the transfer and all corresponding DIF files.

Process Updates:

The resources, personnel, and functions of the National Background Investigations Bureau (NBIB), which was previously under the U.S. Office of Personnel Management (OPM), were transferred to DCSA effective October 1, 2019. As of that date, the background investigations process previously carried out by NBIB is carried out by DSCA and all investigative records previously owned by OPM are now owned by DCSA. The legacy IT systems housing the investigative records are, at the time of the MOU, owned and operated by OPM. DCSA has a service level agreement with OPM for the continued use and support of the OPM IT systems in support of background investigations conducted by DCSA. If at any time during the period of the MOU OPM transfers ownership of the IT systems supporting this eDelivery process to DCSA, the MOU agreement shall continue to remain valid as specified in section 10 of the MOU.

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

☒ Yes
☐ No

2.3 Privacy Office Review

Name of Reviewer	Drew Kuchinski
Date Reviewed	08/09/2021
Expiration Date	08/09/2022
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

Enter description here.