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

{Personnel Security Investigation Solution}
({PSIS})

03/20/2019

1 Privacy Point of Contact

Name	Dominique Rice
Title	Information System Security Officer (ISSO)
Phone	202-326-4000 x3485
Email	Rice.Dominique@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 *(please detail in question 9)*
Personnel Security Investigation System (PSIS)	PSIS is a background investigation and security clearance case management system.	Yes	PBGC-12: Personnel Security Investigation Records	PBGC's authority to collect information from you is derived from: 29 U.S.C. § 1302; 5 U.S.C. § 3301; 44 U.S.C. § 3101; Exec. Order No. 10,450; Exec. Order No. 10,577; Exec. Order No. 12,968; Exec. Order No. 13,467; Exec. Order No. 13,488; Exec. Order No. 13,764; 5 C.F.R. § 5.2; 5 C.F.R. §§ 731-732, and 736; 5 C.F.R. § 1400; OMB Circular No. A-130 (Revised July 27, 2016); Federal Information Processing Standard 201; and	No

				Homeland Security Presidential Directive 12.	
eDelivery	eDelivery is an electronic solution hosted by OPM. It provides PBGC's Human Resource Department (HRD) 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 from you is derived from: 29 U.S.C. § 1302; 5 U.S.C. § 3301; 44 U.S.C. § 3101; Exec. Order No. 10,450; Exec. Order No. 10,577; Exec. Order No. 12,968; Exec. Order No. 13,467; Exec. Order No. 13,488; Exec. Order No. 13,764; 5 C.F.R. § 5.2; 5 C.F.R. §§ 731-732, and 736; 5 C.F.R. § 1400; OMB Circular No. A-130 (Revised July 27, 2016); Federal Information Processing Standard 201; and Homeland Security Presidential Directive 12.	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)

PSIS is a background investigation and security clearance query application. This application enables HRD to update and query relevant information about employees and contractors to track the status of background investigations and security clearances. eDelivery provides HRD with the ability 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.

PII will be collected via hard-copy and entered into PSIS by system administrators. Some information will be collected from the Federal Personnel and Payroll System (FPPS) via manual upload by PSIS system users. Other information, such as UPN and AD-ID, are pulled from other systems (General Services Administration (GSA) reports and Active Directory). eDelivery and Personnel Investigation Processing System (PIPS) data is collected from the National Background Investigations Bureau (NBIB) systems via the ConnectDirect File Transfer Protocol (FTP) client. The eFile module allows external users to access the system with limited use. Users will be able to securely upload documents to their respective case files and view where their cases are in the workflow. *Individual* *Federal Agency* *Phone* *Website* *From another information system*

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

N/A

that document.

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date

System Users	7-10	Manager/COR and PSIS Administrator	Create, Read, Write, Update.	08/06/2018
System Administrators	1-3	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete	08/06/2018
Third Party Contractor	As requested only	Federal PSIS Administrator	Create, Read, Write, Update, Delete	N/A

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- security guards, key entry, locked file cabinets, secured facility, closed circuit television, cipher locks, identification badges, and locked offices

Technical Controls- password protection, network firewalls, unique user identification names, encryption, intrusion detection system, personal identity verification card access, and public key infrastructure certificates

Administrative Controls- periodic security audits, backups secured off-site, encryption of backups containing sensitive data, methods to ensure that only authorized personnel have access to PII, mandatory on-boarding training for security, privacy, and records management, annual refresher training for security, privacy, and records management, and role-based training.

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 used to track background investigations of federal and contractor personnel and retrieve completed background investigations from OPM to support the suitability determination process 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 system administrator manually downloads files from the eDelivery interface and places them on PBGC network. PSIS will soon connect directly to the OPM Server in order to pull the background investigation files to the PBGC DMZ sftp Server through Connect Direct Software.

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

☒ Yes
☐ No

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	4/3/19
Expiration Date	4/3/20
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.

2.4 Signatures and Approval

Information System Owner/Information Owner	
Name:	John Goldsby
Dept/Office:	HRD
Phone: 202-326-4000 x 3237	
EmailGoldsby.John @pbgc.gov	
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	
Date signed	4/3/2019

Authorizing Official	
Name: Arrie Etheridge	
Dept/Office:	HRD
Phone: 202-326-4000 x3728	
Email:Etheridge.Arrie @pbgc.gov	
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	
Date signed	4.3.19

Chief Privacy Officer	
Name:	
I certify that I have reviewed this PIA and have fully considered the privacy risks that this system creates.	
Signature	
Date signed	4/3/19

This page is for internal routing purposes of documentation of approvals. Upon final approval, this page <u>must</u> be removed prior to publication of the PIA.