Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Information Technology Infrastructure Operations Department (ITIOD)

Personnel Security Investigation Solution (PSIS)

PIA

08/03/2020

1 Privacy Point of Contact

Name	James Kitchel
Title	Information Owner
Phone	202-229-3756
Email	Kitchel.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 externally *(please detail in question 9)*?
Personnel Security Investigation System (PSIS)	The Personnel Security Investigation Solution (PSIS), an entellitrak web-based application, is hosted by MicroPact Inc, a certified FedRAMP service provider. PSIS is a background investigation and security clearance case management system.	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	No

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 externally *(please detail in question 9)*?
				Presidential Directive 12.	
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	No

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 externally *(please detail in question 9)*?
				Presidential Directive 12.	

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. eDelivery provides ITIOD with the ability to securely retrieve investigative files to process, adjudicate, and track the status of PBGC background investigation cases.

Under the guidance of PBGC's Risk Management Framework, this PIA is being updated as part of the annual recertification. PSIS is an existing system and this PIA is a living document and may be updated if changes are to occur.

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 Defense Counterintelligence and Security Agency (DCSA) 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.

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

In upcoming enhancements, as opposed to a manual upload to PSIS, the GSA file is planned to be pushed directly from USAccess through a System Infrastructure Provider (SIP) to PSIS. The data model for this enhancement includes new data fields, but no new data types. Below are the drafts of the new data fields that are being proposed.

Table Name	Data Element Name	Data Element Type	New	Source
Investigation Files	Associated Case	Lookup/Dropdown	New	Automatic System Entry
HSPD-12	Card Serial Number	Text	New	USAccess
HSPD-12	Sponsorship Status	Lookup/Dropdown	New	USAccess
HSPD-12	Enrollment Status	Lookup/Dropdown	New	USAccess
HSPD-12	Adjudication Status	Lookup/Dropdown	New	USAccess
HSPD-12	Date PIV Printed	Date	New	USAccess
HSPD-12	Cert Update	Text	New	USAccess
HSPD-12	Credential Update	Text	New	USAccess
HSPD-12	PIV Shipped Date	Date	New	USAccess
HSPD-12	Tracking Number	Text	New	USAccess
HSPD-12	Comments	Long Text	New	Manual Entry
Case	Case Status	Lookup/Dropdown	New	Automatic System Entry
Case	Assigned Security Assistant	Lookup/Dropdown	New	Manual Entry
Applicant Intake	Fair Credit First Name	Text	New	Manual Entry
Applicant Intake	Fair Credit Last Name	Text	New	Manual Entry
Applicant Intake	Fair Credit Social Security Numb	Text	New	Manual Entry
Applicant Intake	Certifying Signature	Text	New	Manual Entry
Applicant Intake	Fair Credit Needs Correction	Yes/No	New	Manual Entry
Applicant Intake	Fair Credit Review Comments	Long Text	New	Manual Entry
Applicant Intake	Employment Type	Lookup/Dropdown	New	Manual Entry
Applicant Intake	First Name	Text	New	Manual Entry
Applicant Intake	Middle Name	Text	New	Manual Entry
Applicant Intake	Last Name	Text	New	Manual Entry
Applicant Intake	Personal Email Address	Text	New	Manual Entry
Applicant Intake	Street 1	Text	New	Manual Entry
Applicant Intake	Street 2	Text	New	Manual Entry
Applicant Intake	City	Text	New	Manual Entry
Applicant Intake	Country	Lookup/Dropdown	New	Manual Entry
Applicant Intake	State	Lookup/Dropdown	New	Manual Entry
Applicant Intake	Zip Code	Text	New	Manual Entry
Applicant Intake	Phone Number	Text	New	Manual Entry
Applicant Intake	Date of Birth	Date	New	Manual Entry
Applicant Intake	US Citizen	Yes/No	New	Manual Entry
Applicant Intake	Social Security Number	Text	New	Manual Entry
Applicant Intake	Primary Country of Citizenship	Lookup/Dropdown	New	Manual Entry
Applicant Intake	Countries of Citizenship	Multi-Select	New	Manual Entry
Applicant Intake	Birth Country	Lookup/Dropdown	New	Manual Entry
Applicant Intake	Birth State	Lookup/Dropdown	New	Manual Entry
Applicant Intake	Birth City	Text	New	Manual Entry
Applicant Intake	Applicant Info Need Correction	Yes/No	New	Manual Entry
Applicant Intake	Applicant Info Comments	Long Text	New	Manual Entry
Applicant Intake	General Comments	Long Text	New	Manual Entry
Pre-Screening	Submitting Official	Text	New	Manual Entry
Record Check	Record Check Type	Lookup/Dropdown	New	Manual Entry
Record Check	Record Check Request Date	Date	New	Manual Entry
Record Check	Record Check Completion Date	Date	New	Manual Entry
Record Check	Record Check Result	Date	New	Manual Entry
Record Check	Comments	Long Text	New	Manual Entry
RAI	RAI Type	Lookup/Dropdown	New	Manual Entry
eQIP	eQIP Request ID	Text	New	Manual Entry
eQIP	SF Form	Lookup/Dropdown	New	Manual Entry
eQIP	eQIP Initiation Date	Date	New	Manual Entry
eQIP	eQIP Submission Due Date	Date	New	Manual Entry
eQIP	eQIP Complete Date	Date	New	Manual Entry
eQIP	eQIP Rejected Date	Date	New	Manual Entry
eQIP	Created On	Timestamp	New	Automatic System Entry
eQIP	Created By	Lookup/Dropdown	New	Automatic System Entry
eQIP	Updated On	Timestamp	New	Automatic System Entry
eQIP	Updated By	Lookup/Dropdown	New	Automatic System Entry
eQIP Extension	eQIP Extension Grant Date	Date	New	Manual Entry
eQIP Extension	eQIP Extension Due Date	Date	New	Manual Entry
eQIP Extension	Comments	Long Text	New	Manual Entry
eQIP Extension	Created On	Timestamp	New	Automatic System Entry
eQIP Extension	Created By	Lookup/Dropdown	New	Automatic System Entry
eQIP Extension	Updated On	Timestamp	New	Automatic System Entry
eQIP Extension	Updated By	Lookup/Dropdown	New	Automatic System Entry

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.

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, information captured by eDelivery, which includes Personally Identifiable Information (PII), 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:

Table 1: PSIS

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Manager Reviewer	2	Manager/COR and PSIS Administrator	Read, Write, Update, Search	Annually
System Administrators	1	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Security Specialist	2	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Adjudicator	2	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Admin Read Only	1	Manager/COR and PSIS Administrator	Read, Search	Annually
Federal Team Member	5	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Search	Annually
Security Assistant	2	Manager/COR and PSIS Administrator	Create, Read, Write, Update, Delete, Search	Annually
Efile	0	Manager/COR and PSIS Administrator	None	Annually
OIG	0	Manager/COR and PSIS Administrator	Read, Search	Annually

PSIS user roles are subject to change in the enhancements that are underway. The following roles have been proposed for PSIS: Security Assistant, Security Specialist, Fed Team Member, Adjudicator/Fed Team Lead, System Administrator, and Super User. Security Assistant, Fed Team Member, and Super User will be new roles.

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.

   The details of the security control implementations are documented in the System Security Plan(SSP).

PSIS physical security controls employed to secure the PII in the system include:	**Related Control Family**	**Inheritance(CCP or CSP)**
1. Security guards	PE-3 Physical Access Control	WSD and MicroPact
2. Key entry	PE-2 Physical Access Authorization	
3. Locked file cabinets	MP-2 – Media Storage (Inherited from CSP)	MicroPact
4. Secured facility	PE	WSD and MicroPact
5. Identification badges	PE-2	
6. Locked offices	PE	

PSIS technical security controls employed to secure the PII in the system include:	**Related Control Family and control example**	**Inheritance(CCP or CSP)**
1. Password protection	AC, AT (AC, AT Family)	MicroPact, ECD
2. Virtual Private Network	AC-17 (AC Family)	MicroPact, ITIOD
3. Firewalls	SI-7 (SI Family)	MicroPact, ITISGSS
4. Unique user identification names	IA (IA Family)	ITISGSS, MicroPact, ECD
5. Encryption	SC-12 (SC Family)	MicroPact, ITISGSS
6. Intrusion Detection Systems	SI-04 (SI Family)	MicroPact, ITISGSS
7. Personal Identity Verification (PIV) card access	IA-2(12), IA-5(3) (IA Family)	ITISGSS, MicroPact, ECD
8. Public Key Infrastructure (PKI) Certificates	SC-17 (SC Family)	MicroPact, ITISGSS

PSIS administrative security controls employed to secure the PII in the system include:		**Inheritance(CCP or CSP)**
1. Periodic security audits	AU Family	MicroPact
2. Backups secured off-site, encryption of backups containing sensitive data	SC, CP Family	MicroPact
3. Regular monitoring of user activity	AU Family	MicroPact
4. Methods to ensure that only authorized personnel have access to PII	AC Family	MicroPact
5. Annual refresher training for security, privacy, and records management	AT Family	ECD
6. Mandatory on-boarding training for security, privacy, and Records management personnel		
7. 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 conduct background investigations of federal and contractor personnel and retrieve completed background investigations from DOD to support the suitability determination process of federal and contractor personnel.

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 6/22/2020.

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	Gregory Armstrong
Date Reviewed	August 4, 2020
Expiration Date	August 3, 2021
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.