

Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)



Protecting America's Pensions

**Office of Management and Administration
Government to Government (OMAG2G)**

HRMS (FPPS, FPPS DataMart, eOPF, MHM, WTTS/EODS, FedTalent)

06/24/2019

1 Privacy Point of Contact

Name	Levy Nchotu
Title	Information System Security Privacy Officer
Phone	202-326-4000, Ext. 6139
Email	Nchotu.Levyt@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

<i>Name of component</i>	<i>Describe the component (1 or 2 sentences)</i>	<i>Does this component contain PII</i>	<i>In what system of records (SORN) is this information stored</i>	<i>What is the Legal Authority for collection of this information</i>	<i>Does this system share PII internally (please detail in question 9)</i>
<i>Federal Personnel/Payroll System (FPPS)</i>	<i>FPPS provides personnel and payroll support to numerous agencies. The system is customer-driven, creating and generating personnel transactions, enabling agencies to maintain records electronically.</i>	<i>Yes</i>	<i>OPM/GOVT-1- General Personnel Records</i>	<i>5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107</i>	<i>Yes</i>
			<i>OPM/GOVT-2- employee Performance File System Records</i>	<i>1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107.</i>	
			<i>PBGC-3- Employer payroll leave and attendance record</i>	<i>29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C. 5501-5584.</i>	
			<i>OPM/GOVT-5- Recruitment, Examining and Placement Records</i>	<i>5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.</i>	
			<i>OPM/GOVT-6- Personnel Research and Test Validation Records</i>	<i>5 U.S.C. 1303, 3301, and 4702.</i>	
			<i>OPM/GOVT-7- Applicant Race, Sex, National Origin and</i>	<i>5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11),</i>	

			<p><i>Disability Status Records</i></p> <p><i>and 15D (11); Uniform Guidelines on Employee Selection Procedures (1978); 43 FR 38297 et seq. (August 25, 1978); 29 CFR 720.301; and 29 CFR 1613.301.</i></p>		
			<p><i>OPM/GOVT-9- File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints</i></p> <p><i>5 U.S.C. 5103, 5112, and 5115 for classification appeals, 5346 for job grading appeals, and 5366 for retained grade or pay appeals; 29 U.S.C. 204(f) for FLSA claims and complaints; 31 U.S.C. 3702 for compensation and leave claims; and U.S.C. 5581, 5582, and 5583 and 38 U.S.C. 5122 for disputes concerning the settlement of the account for a deceased Federal civilian officer or employee.</i></p>		
<i>FPPS DataMart</i>	<i>FPPS DataMart is a tool used by HRD to generate business intelligence and analytics reports from FPPS and WTTS.</i>	<i>Yes</i>	<i>OPM/GOVT-1- General Personnel Records</i>	<i>5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as</i>	<i>Yes</i>

				amended by 13478, 9830, and 12107	
			<i>OPM/Govt-2- Employee Performance File System Records</i>	<i>1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107.</i>	
			<i>PBGC-3- Employer payroll leave and attendance record</i>	<i>29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C. 5501- 5584.</i>	
			<i>OPM/GOVT-5- Recruitment Examining and Placement Records</i>	<i>5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.</i>	
			<i>OPM/GOVT-6- Personnel Research and Test Validation Records</i>	<i>5 U.S.C. 1303, 3301, and 4702.</i>	
			<i>OPM/GOVT-7- Applicant Race, Sex, National Origin and Disability Status Records</i>	<i>5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); Uniform Guidelines on Employee Selection Procedures (1978); 43 FR 38297 et seq. (August 25, 1978); 29 CFR 720.301; and 29 CFR 1613.301.</i>	

			<i>OPM/GOVT-9- File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints</i>	<i>5 U.S.C. 5103, 5112, and 5115 for classification appeals, 5346 for job grading appeals, and 5366 for retained grade or pay appeals; 29 U.S.C. 204(f) for FLSA claims and complaints; 31 U.S.C. 3702 for compensation and leave claims; and U.S.C. 5581, 5582, and 5583 and 38 U.S.C. 5122 for disputes concerning the settlement of the account for a deceased Federal civilian officer or employee.</i>	
<i>FedTalent</i>	<i>FedTalent is PBGC's Learning Management System used to support Computer-Based Training and collaborative learning for PBGC federal employees and contractors. It is a software tool used to store and manage online training.</i>	<i>No</i>	<i>N/A</i>	<i>N/A</i>	<i>No</i>
<i>Electronic Official Personnel Folder (eOPF)</i>	<i>eOPF is an automated system used by federal employees to manage their official personnel files online. eOPF retains specific personal data such as</i>	<i>Yes</i>	<i>OPM/GOVT-1- General Personnel Records</i>	<i>5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107</i>	<i>Yes</i>

	<i>payroll, performance records, awards and attendance time.</i>		<i>OPM/GOVT -2- Employee Performance File System Records</i>	<i>1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107.</i>	
			<i>OPM/Govt – 3- Records of Adverse Actions, Performance Based Reduction in Grade Removal Action and Termination of Probationers</i>	<i>5 U.S.C. 3321, 4303, 7504, 7514, and 7543.</i>	
			<i>OPM/GOVT-7- Applicant Race, Sex, National Origin and Disability Status Records</i>	<i>5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); Uniform Guidelines on Employee Selection Procedures (1978); 43 FR 38297 et seq. (August 25, 1978); 29 CFR 720.301; and 29 CFR 1613.301.</i>	
			<i>OPM/GOVT-10- Employee Medical File System Record</i>	<i>Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 33, and 63.</i>	
<i>Monster Hiring Management System (MHM)</i>	<i>MHM is an applicant tracking system used by HR Specialist to create job vacancy announcements, review, rank, and rate applicants online throughout the hiring process.</i>	<i>Yes</i>	<i>OPM/GOVT-5 – Recruitment, Examining and Placement Records</i>	<i>5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532,</i>	<i>Yes</i>

				<i>and 5533, and Executive Order 9397.</i>	
<i>Workforce Tracking and Transformation System/Entry On-duty System (WTTS/EODS)</i>	<i>Workforce data provided by the WTTS system assists in all phases of workforce planning and facilitates the security management of on and off-boarding of personnel. EODS provides a library of on-line forms to be filled out by a federal new hire. The forms are prefilled with information entered by the selectee during his/her application process.</i>	<i>Yes</i>	<i>OPM/GOVT-1 – General Personnel Records</i>	<i>5 U.S.C. 301,1302, 2951, 3301, and Executive Order 9830</i>	<i>Yes</i>
			<i>OPM/GOVT-5 – Recruitment, Examining and Placement Records</i>	<i>5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.</i>	
			<i>OPM/GOVT-7- Applicant Race, Sex, National Origin and Disability Status Records</i>	<i>5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); Uniform Guidelines on Employee Selection Procedures (1978); 43 FR 38297 et seq. (August 25, 1978); 29 CFR 720.301; and 29 CFR 1613.301.</i>	
			<i>OPM/GOVT-9- File on Position Classification Appeals, Job Grading Appeals</i>	<i>5 U.S.C. 5103, 5112, and 5115 for classification appeals, 5346 for job grading appeals, and 5366 for retained grade or pay appeals; 29 U.S.C. 204(f) for FLSA claims and</i>	

				<i>complaints; 31 U.S.C. 3702 for compensation and leave claims; and U.S.C. 5581, 5582, and 5583 and 38 U.S.C. 5122 for disputes concerning the settlement of the account for a deceased Federal civilian officer or employee.</i>	
--	--	--	--	--	--

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)

In early 2019, PBGC Office of Management and Administration (OMA), which includes Budget Department, Human Resources Department (HRD), Quality Management Department (QMD), and Workplace Solutions Department (WSD), reorganized all its current authorizing boundaries. Instead of organizing boundaries by departments or function, the new authorizing boundaries are organized by system operators, such as Government to Government (G2G), Federal Risk and Authorization Management Program (FedRAMP) Certified Cloud Service Provider (CSP), external service provider, and internally operated. As a result:

A new authorizing boundary and Cyber Security Assessment and Management (CSAM) space named OMA Government to Government (OMAG2G) was created, and an Authorized to Use (ATU) is in progress to be completed by 06/28/2019. The OMAG2G authorizing boundary will include HRMS as a child/sub-system.

HRMS consists of a suite of federal shared systems, applications, and Web-based programs utilized by PBGC. All HRMS subsystems are owned and hosted by third-party agencies/vendors — the Department of the Interior (DOI) and Office of Personnel Management (OPM).

DOI hosts the following systems:

- *Federal Personnel/Payroll System (FPPS)*
- *FPPS DataMart*
- *FedTalent Learning Management System*
- *Monster Hiring Management System (MHM)*
- *Workforce Tracking and Transformation System (WTTS)/Entrance on Duty System (EODS)*

OPM hosts the following systems:

- *Electronic Official Personnel Folder (eOPF)*

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.

1. *The system collects PII from federal employees.*
2. *PII is collected through online systems and federally issued paper forms.*
3. *There is a Privacy Act statement on most of the federal forms utilized by PBGC and at the initial jump page of the online systems. Privacy and HRD will continue to collaborate in the development of privacy statements needed for at least two of the forms that collect PII used by HRD.*
4. *Applicants and current Federal employees are given the opportunity to decline to provide their information to include sensitive and or PII, by not submitting their information for the employment opportunity. Declining to provide their information simply means that the individual chooses not to participate in the hiring process for employment opportunity to include payroll, personnel and benefit requirements.*

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.

PBGC HRMS subsystems (FPPS, FPPS DataMart, MHM, WTTS/EODS, FedTalent and eOPF) leverage all available DOI, and OPM privacy controls. (AP-01, AP-02, AR-01, AR-04, AR-06, AR-07, DI-02, SE-01, SE-02, TR-02, TR-03)

Each party is responsible for compliance with the Privacy Act and related privacy laws, regulations, and policies, including publication of Privacy Act SORNs, for their respective records in this system where applicable, and the collection, use, maintenance and dissemination of PII consistent with the party's agency privacy policy. The access, use and sharing of Pension Benefit Guaranty Corporation (PGBC) data shall be governed by approved sharing agreements as established between DOI and Pension Benefit Guaranty Corporation (PGBC), and the purpose and proposed uses of the data shall be consistent with the applicable SORN. All requests for records or information, Privacy Act notification, access and amendment, Privacy Act complaints, and requests made under the Freedom of Information Act (FOIA) will be the responsibility of the Client/Information Owner. Privacy Impact Assessments (PIA) were conducted and approved on October 1, 2012 for the DDC, and September 30, 2015 for FPPS by DOI to address the privacy implications and the privacy controls implemented to safeguard the information and ensure the confidentiality, integrity, and availability of the information contained in this system. System administrators from

both parties will comply with appropriate privacy controls and safeguards to protect both parties' data and information systems during the transfer of data between systems. Each party will take appropriate action to ensure all technical, physical, and administrative controls are in place to protect data and ensure system security, and will expeditiously notify the designated counterpart of any changes requiring immediate attention.

5. For the user roles in the system:

Table 1 FPPS

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Administrator	2	Vincent McKinney	Read, Write, Execute	Annually
Concurrer	22	Vincent McKinney	Read, Write	Annually
Initiator	48	Vincent McKinney	Read, Write	Annually
Requestor	13	Vincent McKinney	Read, Write	Annually
Authorizer	83	Vincent McKinney	Read, Write	Annually
SC1-SPO	34	Vincent McKinney	Write	Annually
SC2-SPO LGAP	6	Vincent McKinney	Write	Annually
Time and Attendance	6	Vincent McKinney	Write, Execute	Annually
EEO	10	Vincent McKinney	Read	Annually

Table 2 FPPS DataMart

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Consumer	4	Doug Beaver	Read	Annually
Authorizer	3	Doug Beaver	Read, Write	Annually
Scheduler	2	Doug Beaver	Read, Write, Execute	Annually

Table 3 FedTalent

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Site Administrator	5	Helen Castle	Read, Write, Execute	Annually
General User	~2500	Helen Castle	Read	Annually
Training Specialist	3	Helen Castle	Read, Write	Annually
Supervisor	3	Helen Castle	Read, Write	Annually

Table 4 eOPF

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Investigator	6	Vincent McKinney	Read	Annually
Super User	43	Vincent McKinney	Read, Write	Annually
General User	~1000	Vincent McKinney	Read	N/A

Table 5 MHM

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Analytics	5	Vincent McKinney	Read, Write	Annually
HR Specialist	13	Vincent McKinney	Read, Write	Annually
User Management	5	Vincent McKinney	Read, Write, Execute	Annually

Table 6 WTTS/EODS

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
EEO	8	Vincent McKinney	Read, Write,	Annually
HR Representative	87	Vincent McKinney	Read, Write	Annually
Manager (IBC)	1	Vincent McKinney	Read, Write, Execute	Annually
Security Administrator	10	Vincent McKinney	Read, Write	Annually
Supervisor	26	Vincent McKinney	Read, Write	Annually

6. Does the System leverage the Enterprise Access Controls?

Yes

No

The only subsystem of HRMS that leverages Enterprise Access Controls through GetITALL is FedTalent.

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

HRMS physical security controls:

HRMS leverages DOI and PBGC physical security controls employed to secure the PII in the system. These controls include security guards, key entry, locked file cabinets, secured facility, identification badges, locked offices.

HRMS technical security controls:

HRMS leverages DOI and PBGC technical security controls employed to secure the PII in the system. These controls include - password protection, Virtual Private Network, firewalls, unique user identification names, encryption, intrusion Detection Systems, Personal Identity Verification (PIV) card access, Public Key Infrastructure (PKI) Certificates.

HRMS administrative security:

HRMS leverages some of the administrative security controls employed to secure the PII in the system from DOI and PBGC. The leverage controls include – records management, backups secured off-site, role-based training, and methods to ensure that only authorized personnel have access to PII.

As additional administrative internal controls, HRMS IOs review system audit logs, regularly monitor user's activity, conduct annual user role certification to maintain system access and conduct PBGC specific role-based training. PBGC Quality Management Department (QMD) manages mandatory on-boarding training for security, privacy, and records management for all federal and contract personnel.

DOI has implemented the applicable privacy controls for their systems under NIST SP 800-53 rev. 4. PBGC has reviewed documentation of the assessment of these controls.

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.

Intended use of the PII:

Collectively, these systems use PII to assist PBGC to accomplish the following business processes: hiring, onboarding, processing personnel actions, processing benefits, creating reports, and managing employee records.

The PII in FPPS is used to facilitate payroll, garnishments, and special appointment programs and to ensure that personnel and payroll actions processed for individuals are properly reported to the appropriate financial entities and the Office of Personnel Management.

The purpose of PII in FPPS DataMart is to track the processing of personnel actions in FPPS and to meet agency reporting requirements.

eOPF is a digital re-creation of an employee's paper personnel folder which spans the lifecycle of a federal employee's job tenure, and thus PII exists on specific personnel forms i.e. SF-50, S-52, Benefits, etc.

The PII in WTTS/EODS facilitates a centralized and standardized automated business capabilities for the on-boarding process of new and transferring employees, provides secure system access for new hires to complete on-line forms, and sends forms directly to FPPS, and tracks SF-52 actions.

The PII in MHM is used to create job vacancy announcements; review, rank, and rate applicants online.

FedTalent contains no PII.

Steps to Limit PII:

To limit the collection of PII, HRD only utilizes the appropriate federal and agency specific forms and authorized supporting documentation for the collection of PII. HRD personnel regularly reviews PBGC-specific forms for appropriate collection of PII. Privacy and HRD collaborate to minimize the collection of PII necessary to perform agency functions.

Reasons the PII is necessary and relevant:

These collective systems use PII information to assist PBGC with hiring, onboarding, processing of personnel actions, benefits, training, and employee records management from all prospective and new employees within PBGC. WTTS/EODS uses PII to facilitate the management of on and off boarding of personnel. FPPS DataMart collects PII for tracking the processing of personnel actions. The collection and use of SSNs are necessary to verify employment eligibility and to allow employees to receive pay, pay taxes, obtain benefits and enroll in federal financial and benefit programs to include direct deposit, beneficiary forms, etc.

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.

Flow of Data in the system:

PII is shared with PBGC's HRD and PBGC's Payroll Travel Office. Data is shared internally through HRMS integration data feeds such as FPPS, WTTS, MHM, FPPS DataMart, EODS, eOPF. Additionally, information contained in this system may be relied upon by FOD systems, such as WebTA and Employee Express. The Interior Business Center (IBC) facilitates the electronic data feeds through daily, weekly and or biweekly uploads. Data feed is uploaded from PBGC to OMAFedRAMP.

Flow of Data out of the system (within PBGC)

1) Additionally, HRD is sharing non-PII but sensitive data with ITIOD from FedTalent and FPPS via a data feed upload, to include but not limited: federal and contractor names, Employee unique identifier, position title, email addresses, bargaining unit status, grade and step intervals, organization information, EOD and separation date, employee training completion dates and more. An MOU will be created between HRD and ITIOD to address respective roles and outlining ITIOD's responsibilities in the event of a security incident, misuse of data, or breach once data is ingested into ITIOD system(s).

2) Data feed is uploaded from PBGC to OMAFedRAMP systems such as FedHR and PSIS.

3) PII is shared with PBGC's HRD and PBGC's Payroll Travel Office

Flow of Data out of the system (other federal agencies):

1) To disclose information to Department of Interior, IBC as part of the payroll/personnel system to process payroll and benefit payroll deduction for employees via a secure trustee network. This information is shared via HRMS systems FPPS, fax or email.

2) Disclose data contained in the eOPF upon request of a gaining Federal Agency when an employee transfers or separates from PBGC in order to keep the official personnel file intact with its entire work history via a secure internet portal. This information is shared electronically via the eOPF secured system, US mail, email password protected or faxed.

Other third parties:

1) Disclose information to officials of labor organizations recognized under 5 USC ch. 71 when relevant and necessary to their duties and representation concerning personnel policies, practices and matters affecting working conditions.

2) Disclose information to health insurance carriers contracting with OPM for FEHB.

3) Disclose information necessary to the Office of Federal Group Life Insurance (FEGLI) to verify election of insurance or claim payment.

4) To disclose information to education institutions on appointment of recent graduate to a position in the federal service and to colleges, university officials and student loan lenders regarding information about students in Pathways Program, volunteer service and Student Loan Repayment Program.

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

- Yes
- No

Privacy Office Review

Name of Reviewer	Shawn Hartley
Date Reviewed	June 24, 2019
Expiration Date	June 24, 2020
Result	<input checked="" type="checkbox"/> Approved without conditions <input type="checkbox"/> Approved with conditions (see below). <input type="checkbox"/> Denied

(For Privacy Office Use Only)

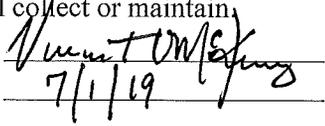
Discuss analysis of risks and compensating controls (or other mitigation steps).

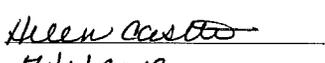
Not Applicable

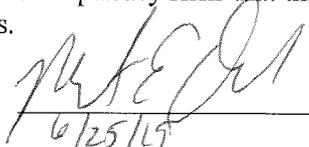
Discuss any conditions on Approval

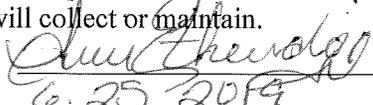
Not Applicable

2.3 Signatures and Approval

Information System Owner/Information Owner	
Name:	Vincent McKinney
Dept/Office:	HRD
Phone:	Ext. 3932
Email:	McKinney.Vincent@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	7/1/19

Information System Owner/Information Owner	
Name:	Helen Castle
Dept/Office:	QMD
Phone:	Ext. 3957
Email:	Castle.Helen@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	7/1/2019

Chief Privacy Officer	
Name:	Margaret Drake
Dept/Office:	OGC
Phone:	Ext. 3358
Email:	Drake.Margaret@pbgc.gov
I certify that I have reviewed this PIA and have fully considered the privacy risks that this system creates.	
Signature	
Date signed	6/25/19

Authorizing Official	
Name:	Arrie Etheridge
Dept/Office:	HRD
Phone:	Ext. 3728
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	6.25.2019

This page is for internal routing purposes – it is solely to document approvals. Upon final approval, this page must be removed prior to publication of the PIA.