

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



**Office of Management and Administration
Government to Government (OMAG2G)
Human Resources Management Systems (HRMS)**

February 2023

1 Privacy Point of Contact

Name	Vincent McKinney
Title	Information System Owner
Phone	202-229-3932
Email	McKinney.Vincent@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.

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)?
Federal Personnel/Payroll System (FPPS)	FPPS provides personnel and payroll support to numerous agencies. The system is customer-driven, creating and generating personnel transactions and enabling agencies to maintain records electronically.	Yes	OPM/GOVT-1- General Personnel Records	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397, as amended by 13478, 9830, and 12107.	Yes
			OPM/GOVT-2- Employee Performance File System Records	5 U.S.C. 1104, 3321, 4305, and 5405, and Executive Order 12107.	
			PBGC-3- Employee Payroll, Leave and Attendance Records	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C. 5501-5584.	
			OPM/GOVT-5- Recruiting, Examining, and Placement Records	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.	
			OPM/GOVT-6- Personnel Research and Test Validation Records	5 U.S.C. 1303, 3301, and 4702.	

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)?
			OPM/GOVT-7- Applicant Race, Sex, National Origin, and Disability Status Records	5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); 29 CFR 720, 1607 and 1613; and 43 FR 38297 Et seq (August 25, 1978).	
			OPM/GOVT-9- File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees	5 U.S.C. 5103, 5112, 5115, 5346 and 5366; 29 U.S.C. 204(f); 31 U.S.C. 3702; 5 U.S.C. 5581, 5582, and 5583 and 38 U.S.C. 5122.	

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)?
FPPS DataMart	FPPS DataMart is a tool used by HRD to generate business intelligence and analytics reports from FPPS and WTTS.	Yes	OPM/GOVT-1- General Personnel Records	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397, as amended by 13478, 9830, and 12107.	Yes
			OPM/GOVT-2- Employee Performance File System Records	5 U.S.C. 1104, 3321, 4305, and Executive Order 12107.	
			PBGC-3- Employee Payroll, Leave and Attendance Records	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C 301 and 5501-5584.	
			OPM/GOVT-5- Recruiting, Examining, and Placement Records	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.	
			OPM/GOVT-6- Personnel Research and Test Validation Records	5 U.S.C. 1303, 3301, and 4702.	

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)?
			OPM/GOVT-7- Applicant Race, Sex, National Origin, and Disability Status Records	5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); 29 CFR 720, 1607 and 1613; and 43 FR 38297 Et seq (August 25, 1978).	
			OPM/GOVT-9- File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees	5 U.S.C. 5103, 5112, 5115, 5346; 29 U.S.C. 204 (f); 31 U.S.C. 3702; and 5 U.S.C. 5581, 5582, and 5583; and 38 U.S.C. 5122.	
FedTalent	FedTalent is PBGC's Learning Management System used to support Computer-Based Training and collaborative learning for PBGC federal	No	N/A	N/A	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 internally (please detail in question 9)?
	employees and contractors. It is a software tool used to store and manage online training.				
Electronic Official Personnel Folder (eOPF)	eOPF is an automated system used by federal employees to manage their official personnel files online. eOPF retains specific personal data such as payroll, performance records, awards, and attendance time.	Yes	OPM/GOVT-1- General Personnel Records	5 U.S.C. 1302, 3301, 301, 2951, 3372, 5 U.S.C 293 et seq. and Executive Orders 9830 and 12107.	Yes
			OPM/GOVT -2- Employee Performance File System Records	5 U.S.C. 1104, 3321, 4305, and 5405, and Executive Order 12107.	
			OPM/GOVT – 3- Records of Adverse Actions, Performance Based Reduction in Grade Removal Actions, and Termination of Probationers	5 U.S.C. 3321, 4303, 7504, 7514, and 7543.	
			OPM/GOVT-7- Applicant Race, Sex, National Origin and Disability Status Records	5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); 29 CFR 720, 1607 and 1613; and 43 FR 38297 Et seq (August 25, 1978).	

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)?
			OPM/GOVT-10- Employee Medical File System Records	Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 33, and 63.	
Monster Hiring Management System (MHM)	MHM is an applicant tracking system used by HR Specialist to create job vacancy announcements and review, rank, and rate applicants online throughout the hiring process.	Yes	OPM/GOVT-5 – Recruiting, Examining, and Placement Records	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.	Yes
Workforce Tracking and Transformation System/Entry On-duty System (WTTS/EODS)	Workforce data provided by the WTTS system assists in all phases of workforce planning and facilitates the personnel security management of on and off-boarding of personnel. EODS provides a library of online 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.	Yes	OPM/GOVT-1 – General Personnel Records	5 U.S.C. 1302, 3301, 301, 2951 and Executive Order 9830.	Yes
			OPM/GOVT-5 – Recruiting, Examining, and Placement Records	5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532,	

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)?
				and 5533, and Executive Order 9397.	
			OPM/GOVT-7- Applicant Race, Sex, National Origin and Disability Status Records	5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11); 29 CFR 720, 1607 and 1613; and 43 FR 38297 Et seq (August 25, 1978).	
			OPM/GOVT-9- File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees	5 U.S.C. 5103, 5112, 5115, 5346; 29 U.S.C. 204 (f); 31 U.S.C. 3702; and 5 U.S.C. 5581, 5582, and 5583; and 38 U.S.C. 5122.	

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).

OMAG2G consists of a suite of federal shared systems, applications, and Web-based programs utilized by PBGC Human Resources Department. All OMAG2G subsystems are owned and hosted by third-party agencies/vendors — the Department of the Interior (DOI) and Office of Personnel Management (OPM). OMAG2G is an existing system, as such the document is going through an annual recertification update.

DOI hosts the following systems:

- Federal Personnel/Payroll System (FPPS)
- DataMart (Oracle Business Intelligence Enterprise Edition (OBIEE))
- FedTalent Learning Management System
- Monster Hiring Management System (HMS)/Position Classification
- 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. HRD collects PII directly from individuals via paper forms or online forms and the Privacy Act Statement is provided at the time of collection.
 - Paper forms: Privacy Act Statement is part of the paper forms. Most of the paper forms PBGC uses are Federal Forms created by other Federal agencies (e.g., OPM, DHS, IRS, etc.).
 - Online forms: When individuals log onto the system to provide PII, the Privacy Act Statement is displayed on the screen. This system is a Software as a Service (SaaS) provided by another Federal Agency. Therefore, this portion of the control is inherited externally.
2. Applicants are given the opportunity to decline to provide their own information 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 that employment opportunity. New hire employees are also given the opportunity to decline providing their own information or by opting to participate in only benefit programs of their choosing. Declining to provide their information will prevent the new hire employee from enrolling in that benefit program.

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 OMAG2G is responsible for all the applicable privacy controls while the Federal service providers are also responsible to implement the privacy controls.

The only control PBGC fully inherited from the Federal service provider, Department of the Interior (DOI), is *DI-02 Data Integrity And Data Integrity Board*.

PBGC has a MOU with DOI. Below is the summary of the privacy portion of the MOU.

“DOI and customer agency are responsible for compliance with the Privacy Act and related privacy laws, regulations, and policies, including publication of Privacy Act SORNs and requests for notification, access or amendment, for their respective records in this system where applicable. The collection, use, maintenance, sharing and disposal of PII must be consistent with the party’s governing SORN(s) and agency privacy policy. The access use and sharing of PBGC data shall be governed by approved sharing agreements as established between DOI and PBGC. 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 PBGC as the Client/Information owner.”

PBGC has an Interagency Agreement (IAA) with OPM. The IAA included the standard privacy clause *“PBGC’s Privacy Clause for Inclusion in IAA’s”*.

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	Write	01/17/2023
Concurren	14	Vincent McKinney	Read, Write	01/17/2023
Initiator	42	Vincent McKinney	Read, Write	01/17/2023
Requestor	3	Vincent McKinney	Read, Write	01/17/2023
Authorizer	83	Vincent McKinney	Read, Write	01/17/2023
SC1-SPO	12	Vincent McKinney	Write	01/17/2023
SC2-SPO LGAP	25	Vincent McKinney	Write	01/17/2023
SPO PROC	42	Vincent	Read, Write	01/17/2023

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
		McKinney		
BlueZone	8	Vincent McKinney	Write, Execute	01/17/2023

Table 2: DataMart

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Consumer	22	Doug Beaver	Read	01/17/2023
Authorizer	8	Doug Beaver	Read, Write	01/17/2023
Scheduler	4	Doug Beaver	Read, Write	01/17/2023
ADM Group	2	Doug Beaver	Read, Write	01/17/2023
Publisher	2	Doug Beaver	Read, Write	01/17/2023

Table 3: FedTalent

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Site Manager	6	Helen Castle	Read, Write, Execute	01/27/2023
General User	2434	Helen Castle	Read	01/27/2023
Program Manager	2	Helen Castle	Read, Write	01/27/2023
Course Creator	2	Helen Castle	Read, Write,	01/27/2023
CSC Help Desk	71	Helen Castle	Read, Write	01/27/2023
Reports Runner	31	Helen Castle	Read, Write	01/27/2023
User Interface Manager	21	Helen Castle	Read, Write,	01/27/2023
Merge User Accounts	2	Helen Castle	Read, Write,	01/27/2023

Table 4: eOPF

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Super User	37	Vincent McKinney	Read	01/17/2023

Table 5: MHM

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Analytics	13	Vincent McKinney	Read, Write	01/17/2023
HR Specialist	21	Vincent McKinney	Read, Write	01/17/2023

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Manage Vacancy Templates	6	Vincent McKinney	Read, Write	01/17/2023
Classification Access	10	Vincent McKinney	Read, Write	01/17/2023
User Management	2	Vincent McKinney	Read, Write	01/17/2023
Selecting Official	162	Vincent McKinney	Read, Write	01/17/2023
UM Access	4	Vincent McKinney	Read, Write	01/17/2023

Table 6: WTTS/EODS

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
EEO	6	Vincent McKinney	Read, Write, Execute	01/17/2023
HR Representative	71	Vincent McKinney	Read, Write	01/17/2023
Manager (IBC)	5	Vincent McKinney	Read, Write, Execute	01/17/2023
Security Administrator	4	Vincent McKinney	Read, Write	01/17/2023
Supervisor	5	Vincent McKinney	Read, Write	01/17/2023

6. Does the System leverage the Enterprise Access Controls?

- ☒ Yes
☐ No

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

OMAG2G physical security controls:

OMAG2G leverages DOI physical security controls employed to secure the PII in the system. These controls include security guards, key entry, and secured facility, etc.

The Human Resources Department (HRD) is the main user of OMAG2G. Access to HRD office is restricted to authorized personnel only.

OMAG2G technical security controls:

OMAG2G leverages DOI technical security controls employed to secure the PII in the system. These controls include password protection, configuration management, contingency planning, audit logging, firewalls, unique user identification names, encryption, intrusion detection systems, and vulnerability scanning, etc.

PBGC is responsible for reviewing and approving PBGC user access requests and performing annual user account recertifications.

OMAG2G administrative security:

For Administrative security controls, OMAG2G fully leverages DOI's incident response controls to secure the PII in the system. Awareness and Training, Incident Response, Personnel Security, Planning, Security Assessment and Authorization (SA&A) controls are hybrid between OMA and DOI. For example, OMA conducts the annual SA&A process and reviews DOI's SA&A package onsite at least annually.

the PII in the system.

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, on-boarding, processing personnel actions, processing benefits, off-boarding, creating reports, and managing employee records.

The PII in FPPS and eOPF is used to facilitate payroll, federal benefits, retirement 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 DataMart is to track the processing of personnel actions in FPPS and to meet agency reporting requirements.

eOPF is an electronic version of the paper OPF and a system for accessing the electronic folder online. The eOPF allows each employee to have an electronic personnel folder instead of a paper 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, Benefit documents, etc.

The PII in WTTS/EODS facilitates a centralized and standardized automated business capability for the on-boarding and off- secure boarding process of new federal employees and separations, provides system access for new hires to complete online forms, and transfer form data directly to FPPS and eOPF if applicable, and tracks SF-52 actions.

The PII in MHM is used to create job vacancy announcements and 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 or the applicable PBGC Department regularly review 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, on-boarding, off-boarding, processing of personnel actions, benefits, and employee records management from all prospective and new employees within PBGC. WITTS/EODS uses PII to facilitate the management of on and off-boarding of federal personnel. DataMart collects PII for tracking the processing of personnel actions. The collection and use of SSNs are necessary to verify federal employment credentialing/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, Office of Information and Technology/Personnel Security Office, and PBGC's Payroll Travel Office. Data is shared internally through OMAG2G integration data feeds such as FPPS, WTTS, MHM, DataMart, EODS, eOPF, and QuickTime. The Interior Business Center (IBC) facilitates the electronic data feeds through daily, weekly, and/or biweekly uploads. Data feed is uploaded from PBGC to OMAG2G.

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

1. To disclose information to the Department of Interior, IBC, as part of the payroll/personnel system to process payroll and benefit payroll deduction for employees via a secure trusted network. This information is shared via OMAG2G systems FPPS, fax, or email.
2. Permanent records and specific disclosed data (SF-75/1150) contained in the eOPF and FPPS when an employee is transferring to the gaining Federal Agency upon written request or separates from PBGC in order to keep the official personnel file intact via a secure internet portal. This information is shared electronically via the eOPF secured system, US mail, email (password protected), or faxed per the gaining Agency's preference.

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 to Office of Personnel Management for retirement or death in service information.
4. Disclose information necessary to the Office of Federal Group Life Insurance (FEGLI) to verify election of insurance or claim payment.
5. 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.

PBGC has a MOU/ISA with DOI.

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

☒ Yes

☐ No

11. If your system collects, Social Security Numbers:

a. Please provide a justification for the collection, use, maintenance, and

HRMS utilizes the authority to solicit, collect, maintain and dispose SSN's provided by law, require interoperability with organizations beyond Pension Benefit Guaranty Corporation to include Interior Business Center, Dept of Treasury, Office of Personnel Management, Dept of Labor, Social Security Administration, Internal Revenue System, Law Enforcement Offices, other Federal, state and local entities.

The leveraged government systems to include FPPS, WTTS, DataMart, FedTalent, EOPF, Monster are used to process personnel and payroll for federal employees according to existing regulatory, statutory, and financial information requirements relating to federal pay, benefits, retirement, recruitment, onboarding, record maintenance entitlements, applicable policies, and procedures. This includes completion of federal forms and specific information shared across external agencies that accurately identifies information.

The FPPS system provides individual earnings notifications to the Department of Treasury for tax reporting purposes via the SSN. The SSN is also used to identify and match federal employee records internal to PBGC and external Federal, state, or local systems described above but not limited. Title 5, US Code section 1104 authorizes OPM to delegate personnel management functions to other Federal Agencies. Thus, the SSN is vital to properly identifying and maintaining records for complaint regulations and identification purposes to process payroll and personnel related matters. With lack of a universal identifier across external systems will delay and or prevent action of the application/request.

Upon reasonable alternative for collection of data other than the SSN, such as cross wide reference or employee identification number, system decommission or changes, or federal wide changes that eliminate the need for SSN use, HRD will require the indefinite use of SSN. HRMS internal standard operating procedures, communications, SSAE report, etc. will be reviewed annually to ensure data is afforded the highest protections practicable through use of appropriate administrative, technical and physical safeguards.

Cited Sources For Data, PII and SSN Collection

- *Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish SSN or TIN, 2) E.O 9397 as amended by E.O. 13478 (November 18, 2008); 3) 5 U.S.C 301; 4) 31 USC Chapter 3511, 3512, 3513; 5) Federal Employee Retirement Law (Chapter 84, Title 5 US Code; 6) the Federal Retirement Group Life Insurance Law (Chapter 87, Title 5 US Code); 7) the Federal Health Benefits Law (Chapter 89, Title 5 US Code); 8) Civil Service Retirement Law (Chapter 83, subchapter iii, Title 5 US Code); 9) Veterans Preference Act 1944; 10) Internal Revenue Code sections 3402(f)(2) and 6109; 11) Privacy Act System of Records Notice (SORN), OPM/CENTRAL 1 Civil Service Retirement and Insurance; 12) Federal Employees Compensation Act 5 U.S.C. 8101; Debt Collection Act; 13) Section 6303 of 5 U.S.C., "Annual Leave Accrual," authorizes collection of information to determine and record service that may be creditable for accrual of annual leave. 14) Part 351.503, 5 C.F.R., "Length of Service," authorizes collection of data to determine and record service that may be creditable for reduction-in-force retention purposes.*

disposal of PII in the form of SSN.

- b. Under which authorized uses, as described in the “Reduction of Use of Social Security Numbers (SSN) in PBGC” policy document?

Based on the *Reduction of Use of Social Security Numbers (SSN) in PBGC* document, there are numerous areas outlined as “Authorized Uses of SSN”. which justify the collection, use, maintenance, and disposal of Social Security Numbers in the OMAG2G HRMS arena.

- b. Security clearance investigation or verification
- c. Interactions with financial institutions
- d. Confirmation of employment eligibility
- e. Administration of Federal Worker’s Compensation
- f. Federal taxpayer identification
- g. Government Data Matching
- h. Oversight work conducted by the OIG

- 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.

Enter description here.

2.3 Privacy Office Review

Name of Reviewer	Shannon Kreshtool
Date Reviewed	2/22/2023
Expiration Date	Twelve months from date of concurrence by Cybersecurity and Privacy Catalog (CPC)
Result	<input type="checkbox"/> Approved without conditions <input checked="" type="checkbox"/> Approved with conditions (see below). <input type="checkbox"/> Denied

(For Privacy Office Use Only)

Not Applicable

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

In the coming year, HRD will work with the Privacy Office and the SSN Reduction Board to work towards eliminating the use of SSNs as the primary identifier for employees.

Discuss any conditions on Approval