Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Office of Management and Administration
Federal Risk and Authorization Management Program
(OMAFedRAMP)

Budget Department Management System (BDMS)

July 2024

1 Privacy Point of Contact

Name	Chuck Kelly
Title	Information System Owner
Phone	202-391-6644
Email	Kelly.Chuck@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)
People Planner	People Planner (PLP) provides the ability to budget and project costs at an employee detail level within the application. This solution allows detailed planning with the ability to incorporate into a dimensional cube providing data transparency from the dimensional model to the individual detailed records.	Yes	OPM SORN GOVT-1 General Personnel Records -88 FR 56058 (8/17/2023)	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107.	No
Microsoft Access Database	BDMS contains a legacy Access database to perform the position management function within the Budget Department. People Planner is replacing the Access database.	Yes	See above	See above	No

| Database extracts from Consolidated Financial System (CFS) and Human Resources Management System (HRMS) | Extracts from CFS and HRMS contain data originating from the Department of Interior's Federal Personnel and Payroll System (FPPS) | Yes | DOI-85, Payroll, Attendance, Retirement, and Leave Records - 83 FR 34156 (July 19, 2018) | 5 U.S.C. 5101, et seq., 31 U.S.C. 3512 | 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).

> BDMS supports a rolling 5-year strategic planning and budgeting process to align resources with PBGC's strategic goals and objectives. BDMS meets all the business requirements of Budget Formulation at PBGC with consideration of the following main goals:
>
> - Automate budget formulation
>
> - Improve data availability
>
> - Generate operating efficiencies
>
> BDMS provides a purpose-built Budget Formulation Solution that enables and automates the formulation and adjustment functions of budget management. It provides real-time budget figure updates across a collaborative, secure environment. It eliminates manual budgeting processes, improves communication and decision support, and increases transparency. All budget data is stored in a central repository with role-based access controls, following the principle of least privilege. The use of workflow automation is also available for all budgeting processes and workflows. Real-time budget status is also available via dashboards to all authorized users based on user roles. The Budget Formulation Solution will have reporting capabilities to help with budget report requirements.
>
> The addition of the People Planner module to BDMS introduces PII. Therefore, this addition is considered a major change to the current authorization of BDMS.
>
> BDMS is a Software as a Service (SaaS) solution by OneStream Software and a subsystem within the OMAFedRAMP authorization boundary.

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 contained within BDMS is loaded manually via a CSV file from OMAG2G Human Resources Management Systems (HRMS).
>
> BDMS does not collect PII from individuals, therefore, providing Privacy Act Statements is not applicable for BDMS.

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.

> BDMS does not inherit any privacy controls from OneStream. All privacy controls are implemented internally by OMA, Common Control Provider (CCP) Privacy Office, or other PBGC CCP.
>
> There is no applicable Service-Level Agreement (SLA), ISA, or MOU for BDMS.

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
Administrator	2	Chuck Kelly	Read, Write	2/16/2024
Global User	11	Chuck Kelly	Read, Write	2/16/2024
BLOs	33	Chuck Kelly	Read, Write	2/16/2024
Department Directors	24	Chuck Kelly	Read, Write	2/16/2024
BPIT/EMC	7	Chuck Kelly	Read	2/16/2024
ITPD	3	Chuck Kelly	Read, Write	2/16/2024
People Planner Super User	3	Chuck Kelly	Read/Write	2/16/2024
People Planner Planner	4	Chuck Kelly	Read/Write	2/16/2024
People Planner Viewer	5	Chuck Kelly	Read	2/16/2024

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, Technical, and Administrative controls that are employed in accordance with NIST SP 800-53 moderate baseline to ensure the data within BDMS. Following are some of the examples.

Physical security controls employed to secure the PII in the system include:
1. Security guards
2. Key entry
3. Locked file cabinets
4. Secured facility
5. Identification badges
6. Locked offices
7. Backups are secured off-site
8. Physical access is only for authorized personnel

Technical security controls employed to secure the PII in the system include:
1. Password protection
2. Virtual Private Network
3. Firewalls
4. Unique user identification names
5. Encryption
6. Intrusion Detection Systems
7. Personal Identity Verification (PIV) card access
8. Public Key Infrastructure (PKI) Certificates
9. System access is only for authorized personnel

Administrative security controls employed to secure the PII in the system include:
1. Periodic security audits
2. Regular monitoring of user's activity
3. Annual refresher training for security, privacy, and records management
4. Mandatory on-boarding training for security, privacy, and records management personnel
5. 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.

> The People Planner module will replace the current Microsoft Access database that is used to facilitate the position management function within the Budget Department with a secure, role-based system. Certain employee-specific information which may be considered PII is either included in the current module or will be included in the future state People Planner module, such as employee name and employee ID. This information is pertinent to the position management function performed by the Budget Department and is used in the formulation and execution of the Corporation's Personnel Compensation and Benefits budget to accurately forecast expected personnel costs. Only the information deemed necessary to carry out the position management, formulation, and execution functions will reside in the People Planning module.

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.

> BDMS receives data from Consolidated Financial System (CFS) (budget actuals from prior years, etc) in the form of CSV files manually shared and imported. Similarly, BDMS will receive data from HRMS (for People Planning) as a manual CSV file-share as well. These are extracted from reports, with some manual processing before import into BDMS. An ISA/MOU is not needed because CFS and HRMS are PBGC-internal systems and the interface is a non-dedicated connection.
>
> BDMS exports data to external agencies (DOL, OMB, Congress) in the form of published reports, which are generated within BDMS and then subject to further review/revision by BD manually. These are submitted via the DEBS system via secure upload. An ISA/MOU is NOT needed because this data reporting/transfer is non-dedicated connection.
>
> The only other form of data interface is reports saved from BDMS for manual sharing within PBGC. In the current state, BDMS has no automated data interfaces with any other systems.
>
> All data interconnections are documented in control CA-3 within CSAM.

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 disposal of PII in the form of SSN?

> BDMS does not collect, use or maintain SSN.

    b. Under which authorized uses, as described in the "Reduction of Use of Social

> N/A

    Security Numbers (SSN) in PBGC" policy document?

    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.

> N/A

2.3 Privacy Office Review

Name of Reviewer	William Black
Date Reviewed	8/1/2024
Expiration Date	Twelve months from date of concurrence by Authorizing Official
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.