

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



**Office of Management and Administration  
Federal Risk and Authorization Management  
Program**

**(OMAFedRAMP)**

**Monster Hiring Management Enterprise (MHME)**

**September 2024**

# 1 Privacy Point of Contact

<b>Name</b>	Johane Pace
<b>Title</b>	Information System Owner
<b>Phone</b>	202-229-3696
<b>Email</b>	Pace.Johane@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)?
Monster Hiring Management Enterprise (MHME)	MHME 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 – Recruitment, 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
Box	Box is an online file sharing tool that allows PBGC and the Office of Personnel Management to exchange reports and information from MHME.	Yes	OPM/GOVT-5 – Recruitment, 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.	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).

Monster Hiring Management Enterprise (MHME) is a Software as a Service (SaaS) provided by Cloud Service Provider (CSP) Monster Government Solutions (MonsterGov). Although MHME is a FedRAMP-authorized product with Package ID FR1711546389, PBGC subscribes to MHME via an Interagency Agreement (IAA) with Department of the Interior (DOI) Interior Business Center (IBC).

MHME is an industry-leading federal talent acquisition product suite, proven to effectively automate and accelerate federal hiring. Fully integrated with USAJOBS, government Human Resources Information Solution (HRIS) systems, and the assessment platform, the hiring suite provides applicants and hiring managers with a simpler and faster way to navigate the federal government's hiring process while remaining secure and fully compliant with federal regulations. MHME contains the Enterprise Suite and the Public Applications Suite.

In limited situations, customers may ask Monster to transmit their own Federal Data to them using Box.com. In some case the data may contain PII elements. Customers may also request that their data be transmitted to third parties, such as EEOC or OMB, at their request. Monster does not transmit any Federal Data using Box without authorization from the customer that owns the data.

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 of the applicants is collected via USAJobs.gov, which is an Office of Personnel Management (OPM) system and interfaces with PBGC’s MHME. Therefore, the responsibility to provide individuals with the Privacy Statement Action resides with OPM.

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 MHME is responsible for any applicable privacy controls. An ISA is not applicable and there is no agreement with OPM for USAJobs.gov, which is used by all federal agencies.

5. For the user roles in the system:

Role Name	# of Users in Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
APPS_Monster_Monster_ANALYTICSACCESS	13	McKinney Vincent, Pace Johane	Read, Write	06/18/2024
APPS_Monster_Monster_HRSPECIALIST	21		Read, Write	06/18/2024
APPS_Monster_Monster_ManageVacancyTemplates	4		Read, Write	06/18/2024
APPS_Monster_Monster_Selecting Official	152		Read, Write	06/18/2024
APPS_Monster_Monster_CLASSIFICATIONACCESS	10		Read, Write	06/18/2024
APPS_Monster_Monster_UMACCESS	3		Read, Write	06/18/2024
APPS_Monster_Monster_ANALYTICSACCESS	13		Read, Write	06/18/2024
Viewer Uploader (Box)	2	MHME	Read. Write	N/A Accounts are managed by cloud service provider.

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.

**MHME physical security controls:**

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

MHME also leverages PBGC Common Control Provider (CCP) physical security controls to secure the facility in PBGC.

**MHME technical security controls:**

MHME leverages CSP 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, vulnerability scanning, etc.

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

**MHME administrative security:**

For administrative security controls, MHME fully leverages the CSP's incident response controls to secure the PII in the system. Awareness and Training, Incident Response, Personnel Security, Planning, and Security Assessment and Authorization (SA&A) controls are hybrid between Office Management Administration (OMA) and the CSP. For example, OMA conducts the annual SPA&A process and reviews the CSP's security package.

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 with the hiring process. The PII in MHME is used to create job vacancy announcements and to review, rank, and rate applicants online.

**Steps to Limit PII:**

To limit the collection of PII, Human Resources Department (HRD) only utilizes the appropriate federal and agency-specific forms and authorized supporting documentation for the 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 the hiring process. 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.

There is data flow between MHME to the PBGC General Support System (GSS) in supporting single sign-on (SSO). Reports about hiring and retention from MHME will be uploaded to Box for non-persistent exchange between OPM and PBGC.

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?

MHME utilizes the authority to solicit, collect, maintain and dispose of SSNs provided by law, require interoperability with organizations beyond PBGC to include Interior Business Center, U.S. Department of the Treasury, Office of Personnel Management, U.S. Department of Labor, Social Security Administration, Internal Revenue System, law enforcement offices, and other federal, state, and local entities.

Until a reasonable alternative exists 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 SSNs. MHME internal standard operating procedures and communications 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.*



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

According to the PBGC Corporate Social Security Numbers (SSN) Reduction Policy, the justification for collection, use, maintenance, and disposal of PII in the form of SSN is:

*d. Confirmation of employment eligibility. Federal statute requires that all persons employed within the United States must provide an SSN or comparable identifier to prove that they are eligible to work for or with the government of the United States.*

- 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

<b>Name of Reviewer</b>	William Black
<b>Date Reviewed</b>	09/04/2024
<b>Expiration Date</b>	Twelve months from date of Privacy Office review
<b>Result</b>	<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