

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



OMA External, FM Interact

10/18/2023

1 Privacy Point of Contact

Name	Leland Chalmers
Title	Information Owner
Phone	202-351-8643
Email	chalmers.leland@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

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.

distinguish or trace an individual's identity, the term PII is necessarily broad.

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.

3 The Components of the System-FM Interact

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)?
FM:Interact	A space management tool.	Yes	GSA/GOV-7	29 U.S.C. 1302, 44 U.S.C. 3101, 5 U.S.C. 301, 80 FR. 64416 (2015).	No
FM:CAD	Can create and publish drawings.	No	N/A	N/A	N/A
FM:CAD Plugin	An add-on to work with FM:CAD	No	N/A	N/A	N/A

3.1 The System as a Whole- FM Interact

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).

The OMAExternal authorizing boundary contains one child/subsystem, FM:Interact. FM:Interact is a Software as a Service (SaaS) provided by FM:Systems (FMS).

FM:Interact System Description

FM:Interact is an integrated web-based facility space management tool that helps PBGC improve workplace management, which includes space, occupancy, assets, and moves. FM:Interact is hosted offsite by FM:Systems in Raleigh, NC, and can be accessed using a secure web browser. FM:Interact components include FM:CAD and the plugin.

FM:CAD is FMS's version of AutoCAD. It is a locally-installed app that lets users create floorplan drawings, mark out office boundaries, and define the types of metadata that will be associated with a floorplan (to be stored in FM:Interact, when the drawing gets "published" there).

FM:CAD's "plugin" is a piece of software that connects FM:CAD to FM:Interact. It is required so that users who have "created" a floorplan in the local FM:CAD tool can "publish" it to the cloud-based FM:Interact repository.

FM:Interact – Allows OMA to electronically manage, track, and communicate space assignments and availability within PBGC. FM:Interact allows OMA to:

- Manage computer aided design (CAD)-type floor plans (including footage, furniture, numbering, and department).
- Show currently vacant/occupied offices/workstations and calculate vacancy rate.
- Track space assignments using an individual's name, office telephone number, room number, square footage, building location, company name, office email, etc.

2. What is the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Low
Availability	Low

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.

FM:Interact does not collect PII directly from individuals. It relies on systems that collect PII directly to provide privacy notice.

PII in FM:Interact is from the PBGC Active Directory. A file is uploaded to FM:Systems utilizing secure file transfer protocol (SFTP). FM:Systems creates and schedules a SQL Server Integration Services (SSIS) package to automatically import the source data on a daily basis.

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.

FM:Interact does not inherit any privacy controls from an external provider. There is no applicable ISA or MOU.

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
System Admin	1	Leland Chalmers	Both	10/03/2023
Power Users	7	Leland Chalmers	Both	10/03/2023
Space Management Users	3	Leland Chalmers	Read	10/03/2023
Space Management Admin	7	Leland Chalmers	Both	10/03/2023
AutoCAD Users	2	Leland Chalmers	Both	10/03/2023

6. Does the System leverage the Enterprise Access Controls?

- Yes
 No

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

Physical Controls:
OMAExternal leverages FM:Systems physical security controls employed to secure the PII in the system. These controls include security guards, key entry, and secured facility.

Technical Controls:
OMAExternal leverages FM:Systems 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.

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

Administrative Security Controls:
OMAExternal fully leverages FM:Systems' 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 OMA and FM:Systems. For example, OMA conducts the annual SA&A process and reviews FM:Systems' SA&A package on site at least annually.

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.

FM:Interact uses PII within the space management tool to facilitate office moves, determine space availability, and departmental assignments.

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.

PII data in FM:Interact is from the PBGC Active directory file uploaded to FM:Systems-specified secure file transfer protocol (SFTP) location. FM:Systems creates and schedules a SQL Server Integration Services (SSIS) package that automatically imports the source data on a daily basis.

Data interconnections are noted in Cyber Security Asset Management (CSAM). Data shared internally within PBGC systems does not require an MOU/ISA.

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?

N/A (FM:Interact does not collect SSN)

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

N/A (FM:Interact does not collect SSN)

- 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 (FM:Interact does not collect SSN)

3.2 Privacy Office Review

Name of Reviewer	Bill Black
Date Reviewed	10/18/2023
Expiration Date	10/18/2024
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.

<i>Enter description here.</i>

Discuss any conditions on Approval.

<i>Enter description here.</i>
