Privacy Impact Assessment for

Enterprise Mainframe (EM)

October 30, 2025

Contact Point
Stuart White
System Owner
CIO/Data Center Group (DCG)

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

Abstract

The Enterprise Mainframe (EM) provides a secure platform for the development, testing, and hosting of several Retirement Services (RS), Healthcare and Insurance (HI), Office of the Chief Financial Officer (OCFO), and administrative support systems that support the mission and goals of the Office of Personnel Management

A Privacy Impact Assessment is required for EM due to EM storing the last four digits of RACF (Resource Access Control Facility – IBM security and access management tool) account users Social Security numbers (SSN).

Overview

The mission of the Office of Personnel Management (OPM) is to build a high quality and diverse Federal workforce, based on merit system principles that America needed to guarantee freedom, promote prosperity, and ensure security. The Enterprise Mainframe (EM) assists OPM in meeting its goals by supporting information systems that serve OPM's principal Program Offices - Retirement Services (RS), Healthcare and Insurance (HI), Office of the Chief Financial Officer (OCFO), and administrative support systems.

The Data Center's mainframe servers form a hybrid infrastructure supporting legacy information systems and new web-based systems on a single highly virtualized architecture.

The EM operates several Federal Continuity Directive Mission Essential Functions (MEF) information systems, which ensure that OPM continues to provide essential functions and meet critical business objectives.

The following program offices have information systems that exist in the two EM environments (primary and contingency sites):

1. Retirement Services (RS) – The Annuity Roll System (ARS) contains several applications that supports federal employees and annuitants'

retirement services and other OPM functions.
2. Healthcare and Insurance (HI) – contains the information systems for Federal Employees Health Benefits (FEHB) Program and the Federal Employees' Group Life Insurance (FEGLI) program.
3. Office of the Chief Financial Officer (OCFO) – The Office of the Chief Financial Officer's Benefits Financial Management System (BFMS) is responsible for the disbursement of payments for many elements of the OPM daily operations.
4. Administrative support systems – The Administrative support systems are responsible for the support and maintenance of OPM's daily activities, as well as its human resources systems with the Data Center Data Exchange Hub used as a centralized service for exporting and importing files into OPM wide applications.

The operational infrastructure OPM Enterprise Mainframe is established at the production site (Boyers, PA) and at the contingency site (Macon, GA). These two operational sites support the three major service sites and smaller sites spread across the United States. At both the production and the contingency sites, the EM infrastructure is comprised of separate sets of independent mainframe hardware and associated peripheral hardware at each site.

EM enforces role-based access control through function groups (user groups that share common access privileges) defined within RACF security. Transmission of EM data over established connections are encrypted through the enforcement of TLS 1.2. Data at rest is protected through RACF which by default, has a "Protect All" setting in place which protects all data using security profiles. Hardware Encryption mechanisms are enabled to accomplish data encryption at rest on mainframe disk and tape storage media.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

44 U.S.C. 3101; EO 9397 (SSN), as amended by EO 13487; and 44 U.S.C. 3534. 4

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

OPM GOVT-1 General Personnel Records Systems; OPM Internal-3 Information Technology, Information System, and Network Activity and Access Records.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

User Identification, Profiles, Authorizations, and Password Files. Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

N/A.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

EM serves as an infrastructure to host several OPM information systems. Information maintained to support the account management of EM RACF accounts are First and Last Name, Last 4 SSN, and Personal Cellphone Number.

2.2. What are the sources of the information and how is the information collected for the project?

This information is provided by the user during the submission of the OPM Form 1665 (Request for OPM Information Technology Access).

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4. Discuss how accuracy of the data is ensured.

The supervisors of the users are required to review and sign the 1665 form prior to submission for approval. The data received supports the account management of the users. The last four of the user's social security number is used to create the account and is expected to remain static. This information is used strictly for account management purposes to verify the identity of the user.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Inaccurate personal information may have been entered into the system

Mitigation: The supervisors of the users are required to review and sign the 1665 form prior to submission for approval. The data received supports the

account management of the users. The last four of the user's social security number is used to create the account and is expected to remain static.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The information is used strictly for account management purposes to uniquely identify the user.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

No.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Yes. The OPM Help Desk are granted limited privileged access to support account management activities, such as the resetting of user passwords.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Disclosure of personally identifiable information (PII) has been and remains a risk to the organization.

Mitigation: Access to the last four of the SSN associated with the user's account is only permitted to authorized privileged users. RACF security and function groups are used to restrict access. Privileged actions, such as account management functions, within EM are audited.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

As part of OPM's account provisioning process, users are required to complete a 1665 (Request for OPM Information Technology Access) form. Within this form, the user must provide the last four of their SSN.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

N/A. The user can decline to provide the requested information. This will also result in the user not being granted access to the Enterprise Mainframe to perform their job.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: N/A

Mitigation: N/A

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Information is destroyed upon creation or update of the final record or when no longer needed for business use. This information is used to uniquely identify and match users to their user accounts.

After 1 year of inactivity for federal users and 90 days of inactivity for contractors, EM (RACF) accounts are archived, all privileges/access are removed, and the last 4 SSN associated with the RACF account is cleared.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: Inactive accounts may have not been archived when they reach the inactivity period threshold.

Mitigation: Access to the Last four of the SSN associated with the user's account remains accessible to only authorized privileged users. RACF security and function groups are used to restrict access. Privileged actions within EM are audited.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

N/A.

6.3. Does the project place limitations on re-dissemination?

N/A.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

N/A.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: N/A.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

Employees generally do not have access to this system. However, RACF Admins and OPM Help Desk employees have access to this information which is strictly used for account management purposes. That said, employees can submit a 1665 Form for new changes.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Any new name change requested by the user would require a new 1665 form request to be submitted. This would be for new changes only, as the individual does not have permissions to view the RACF User Profile.

7.3. How does the project notify individuals about the procedures for correcting their information?

OPM standard procedure is to submit a 1665 form for any individual information changes.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: N/A

Mitigation: N/A

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Access to the Last 4 of the SSN associated with the user's account is only permitted to authorized privileged users. RACF security and function groups are used to restrict access. The OPM Help Desk has limited permissions to what actions they can execute within EM. All account monitoring is in place and audit logs are reviewed and forwarded to the agency SIEM.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

Privileged users must complete OPM's annual Cybersecurity and Privacy Fundamentals Training.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to the Last 4 of the SSN associated with the user's account is only permitted to authorized privileged users. RACF security and function groups are used to restrict access.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

N/A.

Responsible Officials

Stuart White
System Owner
CIO/Data Center Group

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy