USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed "Gender" and "Sexual Orientation" from Biographical Information in accordance with Executive Order 14168, "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government."

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Enterprise Performance Management Application (EPMA)
Program Office	OHRM
Mission Area	Staff Offices > Departmental Administration
CSAM Number	2527
Date Submitted for Review	03/14/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Michele Washington	michele.washington@usda.gov	(202) 205-3369
Information System Security Manager	Lisa McFerson	lisa.mcferson@usda.gov	(202) 720-8599
System/Program Managers	Amelia Ngo	amelia.ngo@usda.gov	(202) 875-4609

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

This PIA is for the Enterprise Performance Management Application (EPMA). EPMA is an enterprise performance management system that utilizes the two-tier rating system as defined by the USDA policy for non-executive performance. This PIA is being conducted in accordance with the EPMA ATU renewal due by 12/31/2026.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The Enterprise Performance Management Application (EPMA) is owned by the Office of Human Resources (OHRM). This system supports OHRM’s mission to promote a competency-based and results-oriented performance culture by aligning all agencies to a single platform and workflow. EPMA allows employees and supervisors to electronically track and manage all performance activities as defined in DR4040-430 in a single online application. A typical transaction in the system involves an employee’s Rating Official, typically their supervisor, documenting the employee’s performance plan, performance appraisal or quarterly conversation that the employee is then responsible for reviewing and acknowledging. The National Finance Center (NFC) is the HR system of record for EPMA, and all employee information reflected in the platform is fed to EPMA by NFC using the Insight platform. No information is shared with other programs or systems beyond EPMA and NFC.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

5 United States Code (U.S.C.) 4302, Establishment of Performance Appraisal Systems

5 Code of Federal Regulations (CFR) Part 430, Performance Management

OPM's approval of the Performance Appraisal System (System)

USDA's Non-Executive Performance Management Program (Program)

1.2. Has Authorization and Accreditation (A&A) been completed for the system?

Yes, 11/1/2024.

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

EPMA is covered under the Government-wide SORNs OPM/GOVT-1, General Personnel Records: *December 11, 2012, 77 FR 73694; modifications published February 2, 2022, 87 FR 5874 and August 17, 2023, 88 FR 56058*; and OPM/GOVT-2, Employee Performance File System Records: and Employee Performance File System Records: *June 19, 2006, 71 FR 35347; modification published February 2, 2022, 87 FR 5874*;

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

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. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☒ Social Security number	☐ Truncated or Partial Social Security number	☐ Driver's License number
☐ Passport number	☐ License Plate number	☐ Registration number
☐ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☒ Employee Identification number	☐ Alien Registration number	☐ DOD ID number
☐ Professional License number	☐ Taxpayer Identification number	☐ Business Taxpayer Identification number (sole proprietor)
☐ Credit/Debit Card number	☐ Business Credit Card number (sole proprietor)	☐ Vehicle Identification number
☐ Business Vehicle Identification number (sole proprietor)	☐ Personal Bank Account number	☐ Business Bank Account number (sole proprietor)
☐ Personal Device Identifiers or Serial numbers	☐ Business Device Identifiers or Serial numbers (sole proprietor)	☐ Personal Mobile number

☐ Health Plan Beneficiary number
☐ Business Mobile number (sole proprietor)
☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)
☐ Business Mailing Address (sole proprietor)
☒ Date of Birth (MM/DD/YY)

☒ Ethnicity
☐ Business Phone or Fax Number (sole proprietor)
☐ Country of Birth

☐ City or County of Birth
☐ Group Organization/Membership
☐ Religion/Religious Preference

☐ Citizenship
☐ Immigration Status
☒ Home Phone or Fax Number

☒ Home Address
☒ ZIP Code
☐ Marital Status

☐ Spouse Information
☐ Children Information
☒ Military Service Information

☒ Race
☒ Nationality
☐ Mother's Maiden Name

☒ Personal Email Address
☒ Business Email Address
☐ Global Positioning System (GPS)/Location Data

☒ Employment Information
☐ Alias (Username/Screenname)
☐ Personal Financial Information (Including loan information)

☒ Education Information
☐ Resume or Curriculum Vitae
☐ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile

☐ Retina/Iris Scans
☐ Video Recording

Distinguishing Features

☐ Palm Prints	☐ Eye Color	☐ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

☐ Vascular Scans	☐ Height	☐ Weight
☐ Scars, Marks, Tattoos	☐ Voice/Audio Recording	

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)	☐ Cell Tower Records (e.g., Logs, User Location, Time)	☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

Specific Information/File Types

☒ Personnel Files	☐ Law Enforcement Information	☐ Credit History Information
☐ Health Information	☒ Academic/Professional Background Information	☐ Civil/Criminal History Information/Police Record
☐ Case Files	☐ Security Clearance/Background Check	☐ Taxpayer Information/Tax Return Information

2.2. What are the sources of the information in the system/program?

All Employee and Position information comes from NFC, the HR system of record.

Performance Information is created by the Rating Official and is specific to the employee and the duties they perform.

2.2.1. How is the information collected?

Employee and Position Information:
On a nightly basis EPMA runs a CRON job that pulls down pre-defined data from reports created in Insight. That data is then loaded into the EPMA database.

Performance Information:
The Rating Official and Employee document this information in the EPMA database by interacting with custom forms and functionality built to capture their specific performance-related activities.

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

No commercial data is used. The system includes a list of Federally owned or licensed buildings for employees to select their primary work location when logging into a Remote Work or Telework agreement. This list comes from GSA's public website.

2.4. How will the information be checked for accuracy? How often will it be checked?

The accuracy of Employee and Position Information is managed by NFC. Agencies have their own processes that allow for corrections if/when needed. Those corrections would be made downstream of EPMA and fed to the system once complete.

Performance Information is checked for accuracy via the built-in workflow of the application. Plans and Appraisals go through approval by Reviewing Officials, typically the employee's 2nd level supervisor. Employees acknowledge performance management activities and information in the system as a final step to ensure its accuracy.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

N/A – EPMA is not 3rd party.

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

N/A

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

Section 3: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Describe that information is fed from the HR System of Record - NFC though Insight. Information is used in relevant EPMA system workflows

Information is maintained via a nightly refresh with Insight

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

No

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Overuse of Information: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Mitigation: By Implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Transparency: Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.

Regular Training: Provide regular training for employees on privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

Notice is given from the HR system of record – NFC.

4.2. What options are available for individuals to consent, decline, or opt out of the project?

None – this is an HR system.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: Privacy Act risks associated with notices include:

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Insufficient Updates: Notices that are not regularly updated to reflect changes in data practices or legal requirements can mislead individuals and result in privacy violations.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Transparency: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.

A link to the USDA Privacy Policy is published in the footer of the application and can be accessed anytime by employees.

If an employee has a question about the privacy policy, or any other performance-related matter, they can contact their USDA agency performance management support at any time.

Section 5: Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

(1) Except as provided in § 293.405(a), performance ratings or documents supporting them are generally not permanent records and shall, except for appointees to the SES and including incumbents of executive positions not covered by SES, be retained as prescribed below:

(i) Performance ratings of record, including the performance plans on which they are based, shall be retained for 4 years;

(ii) Supporting documents shall be retained for as long as the agency deems appropriate (up to 4 years);

(iii) Performance records superseded (e.g., through an administrative or judicial procedure) and performance-related records pertaining to a former employee (except as prescribed in § 293.405(a)) need not be retained for a minimum of 4 years. Rather, in the former case they are to be destroyed and in the latter case agencies shall determine the retention schedule; and

(iv) Except where prohibited by law, retention of automated records longer than the maximum prescribed here is permitted for purposes of statistical analysis so long as the data are not used in any action affecting the employee when the manual record has been or should have been destroyed.

(2) When an employee is reassigned within the employing agency, disposition of records in this system, including transfer with the employee who changes positions, shall be as agencies prescribe and consistent with § 293.405(a).

(3) Appraisals of unacceptable performance, where a notice of proposed demotion or removal is issued but not effected, and all documents related thereto, manual and automated, pursuant to 5 U.S.C. 4303(d) must be destroyed after the employee completes one year of acceptable performance from the date of the written advance notice of the proposed removal or reduction in grade notice. Under conditions specified by an agency, an earlier destruction date is permitted, and destruction must be no later than 30 days after the year is up.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes

Location: www.archives.gov/files/records-mgmt/grs/grs02-3.pdf

Item: 060

Records Description: Administrative grievance, disciplinary, performance-based, and adverse action case files. NOTE: EPMA is specifically and exclusively dealing with the performance-based records.

Disposition Instruction: Destroy no sooner than 4 years but no later than 7 years (see Note 2) after the case is closed or final settlement on appeal, as appropriate.

Note 2: Per OPM, each agency must select one fixed retention period, between 4 and 7 years, for all administrative grievance, adverse action, and performance-based action case files. Agencies may not use different retention periods for individual cases.

Disposition Authority: DAA-GRS-2018-0002-0006

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: Data Breach, Excessive data retention

Mitigation: Data Breach: This risk is mitigated by reducing the amount of PII collected, processed, and stored inside EPMA to only the minimum amount required to successfully complete the performance management process.

This risk is further mitigated by encrypting and hashing PII using a 256-character key. This information is only decrypted at the time it is required based on workflow.

Access to sensitive data is controlled using role-based access and elevated permissions.

Also, implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

Secure Disposal Procedures: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Employee ratings are logged in EPMA and transmitted back to NFC via an electronic interface. NFC is the HR system of record and needs a record of the rating in their system. EPMA posts a PGP encrypted file to NFC's SFTP site. NFC has been provided with EPMA's key to decrypt the file an ingest on their end.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Incorrect Data Exposure

Mitigation: Incorrect Data Exposure: This risk is mitigated by removing the human element of the data-sharing process. The process of sharing data between NFC and USDA was tested and reviewed prior to implementation. Once implemented, the transmission process and destination are automated – removing the risk of transmitting data to an incorrect recipient.

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

N/A – We do not share outside of USDA

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 7: Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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

Employees are part of the workflow of the application and are required to review and acknowledge the content of their performance management plans.

7.2. What are the procedures for correcting inaccurate or erroneous information?

Any corrections to official HR data are done at the agency level following their internal processes for personnel actions.

Any inaccurate or erroneous performance information is resolved between the Rating Official and employee. Rating Officials are allowed to make some corrections side the system. Anything they cannot correct would require a documented support ticket for Enterprise System Administrators to resolve.

7.3. How are individuals notified of the procedures for correcting their information?

Embedded training materials instruct users on what corrections a Rating Official can make. Users are requested to follow their agency support process for any additional questions or issues.

7.4. If no formal redress is provided, what alternatives are available to the individual?

Department Regulation 4040-430 defines the alternatives available to employees that disagree with the content of their performance management plan.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Mitigation: By implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Section 8: Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

8.1. How is the information in the system/project/program secured?

All PII is stored as encrypted and hashed using a 256-character key. This information is only decrypted at the time it is required based on workflow.

Access to sensitive data is controlled using role-based access and elevated permissions.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

Supervisors are automatically granted access to the system due to the performance management requirements of their positions. They receive elevated permissions that allow them complete performance management activities for their direct reports.

Employees are automatically granted access to the system with baseline permissions that allow them to review and acknowledge performance management activities completed by their Rating Officials.

Any access to the system beyond those two groups is protected.

Access to the tool can be granted for agency support personnel pending justification, review, and approval by their supervisor.

Access to the administrative portion of the system can be granted pending justification, review, training, and approval by their supervisor.

8.3. How does the program review and approve information sharing requirements?

Before information is shared, a memorandum of understanding is created and signed by both parties. This covers information sharing internal to USDA. External sharing of information would be covered by the creation of an ISA, though EPMA does not currently share any information with external entities.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

USDA Records Management

USDA Information Security Awareness Training>