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	Military Deposit Retirement System
Program Office	-
Mission Area	DAITO OCFO-NFC
CSAM Number	2723
Date Submitted for Review	10/01/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Nija Enclarde	318-955-1393
Information System Security Manager	Tracy Haskins	202-720-8245
System/Program Managers	Trudy Sandefer	504-426-7663

Abstract

This PIA is for the Military Deposit Retirement Services application (MDRS). MDRS is a modern web-based application that manages all aspects of military buyback for future retirees. This application replaces an entirely manual workflow with a modern toolset.

Overview

The Military Deposit Retirement Services Application (MDRS) will provide users with an improved management process that deals with all aspects of managing Military Buyback Deposits.

In the context of the United States federal government and the Office of Personnel Management (OPM), a military buyback, also known as a military service credit deposit, refers to a program that allows eligible members of the uniformed services (such as the military) to make a financial payment to "buy back" their military service time and credit it towards their federal civilian retirement benefits.

The core concept of MDRS centers around a military deposit "case." A case represents an instance of a military buyback. The case encompasses all the information necessary to manage a military buyback from start to finish. At its core, a case is an accounting of how much an employee owes at any point in time to satisfy their buyback agreement. The case starts with a request from Agency HR on behalf of an employee. This case is then managed over a period of time until it is made inactive by the employee or has been paid in full.

Application users have the ability in MDRS to manage and maintain all aspects of a given military buyback:

- **Search**
  - **Employee** - An employee represents an active federal worker. Employees request a military service buyback for a set of periods. MDRS provides functionality. Upon searching for an employee, a case can be created for them.
  - **Case** – A case search is an easy entry point for managing existing cases.
- **Create Case** – Upon searching for an employee, a case can be created for them. Basic information must be provided to configure the case. The main difference is the retirement system (FERS/CSRS/USERRA) to which the employee belongs.
- **Manage** – A case has several associated elements that require setup and management throughout the military deposit lifecycle. They are:
  - **Service Periods** – A valid case has one or more service periods defining the employee's military time and earnings made. Service Periods then have a calculated amount establishing the beginning balance for the military deposit buyback.
  - **Ledger** – The ledger is the mechanism for tracking the military deposit buyback account balance. It starts with a beginning balance derived from the Service Periods and holds all subsequent transactions. These transactions are a mix of user-entered and system-calculated.
  - **Documents** – Documents on a case are the supporting information that helps define the military deposit buyback case.

  - **Notes** – Notes are user-defined messages providing relevant information about a military deposit buyback case.
- **Review** – MDRS has functionality that assists with data audit and review over time.
  - **History** – Each data version is saved over time so users can see what changes were made and by whom.
  - **Historical Imported Data** – The prior military deposit process was performed manually via over 50,000 spreadsheets stored on a shared drive. The MDRS application team completed a one-time import of that data.
- **Administer** – MDRS provides administration screens to manage users and roles.
- **Automation** – There are MDRS contains automated activities that optimize the application functionality.
  - **Employee Import** – Base employee information is imported into the application nightly so that users do not need to rekey it into the application.
  - **Automated Calculations** – MDRS computes interest amounts and ledger totals throughout the life of a case.
  - **Payment Integration –** Payroll deductions are imported into MDRS and assigned to military deposit cases.
- **Outputs** – The application does generate a few outputs. Users download these PDFs at different points during the Military Deposit lifecycle.
  - **1514** – This document is an OPM requirement created after a military deposit case is completed. It describes the payments and interest paid.
  - **Balance Due Letter** – When requested, this document is used to provide agency HR with the status of a military deposit.

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.

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

Chief Financial Officers Act of 1990 Public Law 101–576.

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

Yes, approved 4/2/2025.

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

OCIO NFC 1 SORN

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.

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

Identifying Numbers:

- Social Security number

Biographical Information:

- Name (Including Nicknames)
- Date of Birth (MM/DD/YY)
- Military Service Information
- Employment Information

Employee information imported:

- SSN
- First/Middle/Last Name
- POI
- DOB
- Department
- Agency

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

The information sources are:

Insight – Insight is used for basic employee information.

OPM – Annually, OPM publishes interest rate documents needed by the MDRS application.

User Input – User input is the primary source of information. Users create and maintain all aspects of military deposit cases.

Legacy MDRS spreadsheets – A one-time import was required to create legacy data in the MDRS application.

How is the information collected?

The information sources are collected in the following manner:

Insight – A batch process nightly connects to Insight, downloads relevant data, and imports it into MDRS.

OPM – OPM provides PDF documents that contain the yearly interest rates. The MDRS team strips the document of the needed information and places it into a format defined by the MDRS application. After proper formatting, the data is imported.

User Input – User Input is collected through a Web Interface.

Legacy MDRS spreadsheets – A complex process was programmed to complete this process. The existing filesystem was scanned, and any documents were uploaded to MDRS. These existing documents, which came in the form of Excel spreadsheets, were then opened by the application, and cases were created based on the data contained within them. All actions of this process were logged for subsequent review.

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

The OPM is publicly available. It is used as a system requirement to automatically calculate the interest accrued on the military deposit cases annually. The OPM interest rate data is required to perform that calculation.

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

The application users check the information. Cases are typically reviewed and updated annually upon interest calculations but are also reviewed when they are closed out.

Does the system/program use third-party websites?

No

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

N/A

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

NONE

Privacy Impact Analysis: Related to characterization of the information.

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

Mitigation: Establish clear definitions for different categories of personal information, helping employees understand how to classify and handle data appropriately.

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.

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

The MDRS application collects this information to remove manual processing of military deposit processing. The data is already being collected manually. The MDRS application modernized the process to provide efficiency.

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

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: Data Breach

Mitigation: This risk is mitigated by reducing the amount of PII collected, processed, and stored inside MDRS to only the minimum required to successfully complete military deposit activities.

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.

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.

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

Initiating a military deposit case starts with the employee and their completed paperwork. MDRS's role in information management occurs after that. NFC customers start the data collection by submitting their paperwork via ServiceNow.

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

None

Privacy Impact Analysis: Related to notice.

Privacy Risk: 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.

Mitigation: Inform users about their rights regarding their personal data, including access, correction, deletion, and the ability to object to processing.

Section 5: Data Retention

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

What information is retained and for how long?

All case management details are retained indefinitely.

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.

Records are retained and disposed of in accordance with approved NARA guidance, NFC Records Control Schedule N1–016–10–7.

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Mitigation: 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.

Section 6: Information Sharing

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

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?

None (There is no transmission of data. The application is for internal NFC use only and is only accessible by the relevant application users).

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: Internal systems can be vulnerable to breaches, compromising PII.

Mitigation: Regularly monitor access logs and conduct audits to detect any unauthorized access or anomalies in data handling.

No information sharing is occurring in the application.

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?

None

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Mitigation: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

No information sharing is occurring in the application.

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.

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

MDRS is a back-office application. Application users are required to authenticate via E-Auth. MDRS contains role-based security to authorize access and delegate the user's privileges.

What are the procedures for correcting inaccurate or erroneous information?

Application users can edit all relevant information.

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

Users have been trained on the MDRS application, which includes correcting erroneous data.

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

N/A

Privacy Impact Analysis: Related to redress.

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

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

Section 8: Auditing and Accountability

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

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

All information is stored in a secure database hosted in the Digital Infrastructure Services Center (DISC).

SSL is used for all data transmissions.

E-Auth is used for authentication.

MDRS contains role-based security for users and roles.

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

Functionally, MDRS contains robust user interface screens to allow user creation/modification/deactivation.

Administratively, MDRS contains integrated help guiding users through the user management process.

How does the program review and approve information sharing requirements?

No information sharing occurs in MDRS.

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

Application is an NFC internal-only application. All NFC employees/contractors are required to take the standard federal privacy training.