



Office of the Chief Information Officer
U.S. DEPARTMENT OF AGRICULTURE

USDA Privacy Impact Assessment

Fiscal Year 2025

Grants Management and Reporting System (GMRS)
National Institute of Food and Agriculture
U.S. Department of Agriculture

Revisions

Date	Version	Notes
03/21/2025	1.0 – 1.8	Legacy PIA Documents
03/21/2025	2.0	Transferred document to a new CPOC Template

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project	4
Mission Area System/Program Contacts	4
Abstract.....	5
Overview	6
Section 1: Authorities and Other Requirements.....	9
Section 2: Characterization of the Information.....	10
Section 3: Uses of the Information.....	12
Section 4: Notice	13
Section 5: Data Retention	14
Section 6: Information Sharing	15
Section 7: Redress	16
Section 8: Auditing and Accountability	17

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Grants Management Reporting System
Program Office	Information Technology Services Division (ITSD)
Mission Area	Research, Education, and Economics (REE)
CSAM Number	1168
Date Submitted for Review	03/21/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Nicole Young	301-504-1075
Information System Security Manager	Andrew Francis	202-336-2101
System/Program Managers	Pratima Boyapati	202-701-3529

Abstract

The Grants Management and Reporting System (GMRS) is a portfolio of applications used to support the grants lifecycle. The system is designed to manage budget outlay; application review and management; award and post-award management; funds management and disbursal; budget reporting; and management of grant and cooperative agreement reviews.

Overview

The Grants Management and Reporting System (GMRS) is an consolidation of components identified below in Table 1 used to support the grants lifecycle. The system is designed to manage budget outlay; application review and management; award and post-award management; funds management and disbursement; budget reporting; and management of grant and cooperative agreement reviews.

The capabilities of the system reinforce accountability to Congress, USDA management, commodity groups, and the public. The system is used to support requirements related to strategic planning and performance assessment and provide electronic delivery of information to a broad user community by monitoring and evaluating agricultural research and extension activities conducted or supported by USDA that will enable measurement of impact and effectiveness of research, extension, and education programs to optimize public access to research information.

System functionalities include the ability to enhance existing NIFA reporting environments by tying together reporting systems across all programs in a central data repository. The system houses a broad range of current and historical data including awards, projects and accomplishment reports to provide state partners and NIFA staff with business information.

Table 1: GMRS System Components

Application	Description
Award Document Repository (ADR)	ADR is NIFA's official electronic grant records repository for noncapacity grant programs. ADR provides functionality to perform records management activities including storage, uploading, search and retrieval and disposition of records.
Aurea ListManager (ALM)	Lyrus is an email distribution system with more than 200 mailing lists of key agricultural stakeholders, including State Agricultural Experiment Station Directors, Cooperative Extension Directors, 1890s institutions, 1994 LGUs, Hispanic Serving Institutions, and more. NIFA uses Lyrus to distribute news about committees, conference registrations, newsletters, documents, and other NIFA updates to these stakeholders.
Communication and Distribution System (CDS)	CDS is Java/J2EE-based software which handles electronic grant application submissions received from NIFA's Gateway Application Connector (GAC). CDS tracks the status of applications, provides error checking and exception handling, notifies applicants that their grant applications have been accepted, and processes grant application data. In addition, it provides a user to view an electronic grant application package as a single bookmarked PDF file. CDS also enables access to grant applications for multiple selected applications, or even for an entire Peer Review Panel or program.
Cherwell	The software provides tracking capabilities to business units in support of NIFA grants administration, specific to ASAP-related account set-up and administration.

Application	Description
Cooperative Research, Education, and Extension Management System (C-REEMS)	Serves as NIFA's primary grants management application for research, education, and extension grant application receipt, review, award, and processing for non-capacity grant programs. C-REEMS is an Oracle Forms/Reports application built on an Oracle database and hosted on a Linux platform.
Current Research Information System (CRIS)	CRIS is an application system maintained by the Applications staff of the Office of Information Technology (OIT) of the National Institute of Food and Agriculture (NIFA) within the U.S. Department of Agriculture (USDA). CRIS serves the USDA, its partner institutions, and the public by enabling the collection and organization of a broad scope of information on agriculture, forestry, food and nutrition from a diverse group of agencies, institutions and organizations. CRIS provides ready access to information through public web accessible data as well as individually requested customized reports and services. CRIS is a centralized database supported by a standardized platform utilizing the Cuadra/STAR file management software as the primary support for the centralized database.
Data Gateway	A publicly available web-based tool reporting tool enabling users to find funding data, metrics and information about research, education and extension activities. This tool also offers standard reports including a Congressional map of NIFA funded projects, recent and historical award data, award trends, and the ability to further refine reports using various predefined filters. The enterprise search technology used in Data Gateway is replicated in REEIS, LMD, and REEport however the Data Gateway serves as an external portal to retrieve project level information.
eGrants Access Manager (eAM)	eAM is a role-based access control tool that works with Active Directory to restrict domain user access to various areas and functionality of the agency's eGrants applications. It provides agency staff insight into user access levels and permissions as well as a full listing of all C-REEMS accounts and the account status. Managers can view additional user information such as roles, contact info, programs and program area information, and change logs.
Financial Processing Application (FPA)	FPA is a Java/J2EE application designed to automate the processing of ASAP (Automated Standard Application for Payment) account setup, funds authorization, disbursement management, and FMMI (Financial Management Modernization Initiative) posting.
Funding Opportunity Linkage System (FOLS)	Provides linkage between funding opportunities on Grants.gov and NIFA program information. FOLS also provides the Grant Application Connector (GAC) system with routing information to ensure NIFA staff has proper access to incoming electronic applications.
Grant Application Connector (GAC)	An application used by program staff to conduct the administrative review of applications received through Grants.gov and accept these applications into our agency for review. Grant applications then move into CDS for secondary review, personnel updates, and tracking.

Application	Description
Grant Management Reporting Application (GMRA)	Provides all staff with access to pre-award and post-award information from C-REEMS, NEDR and other sources for use in grants management administration.
Leadership Management Dashboard (LMD)	A NIFA reporting tool that allows users to access financial and budget information on the agency's programs and grants.
NIFA Enterprise Data Reference (NEDR)	Provides users with access to master reference data on institutions and organizations receiving funding from NIFA.
NIFA Enterprise Web Application Gateway (NEWAG)	A web-based entry point for internal NIFA staff to access most of the applications used to administer, monitor, and report NIFA-administered grants.
NIFA Intranet	An internal website providing access to documents and information relevant to NIFA staff.
NIFA Reporting Portal	The web-based entry point for staff and the public to access a collection of NIFA reporting applications including REEport, POW, and LMD. It also provides additional direct links to other NIFA applications open to the public.
NIFA Website	NIFA's public-facing web presence.
Peer Review System (PRS)	Peer Review System (PRS) is a secured web application built using open source Java/J2EE technologies. The application was designed to support the merit review of competitive grant applications. PRS provides a mechanism to allow panel reviewers to see what grant applications they have been assigned for review, what review criteria is in place for those applications, and to enter review text along with any scoring/rating that is appropriate.
Plan of Work (Institutional Profile)	Enables NIFA to ensure regulatory compliance for the capacity grant programs subject to the Agricultural Research, Education, and Extension Reform Act (AREERA). Provides support for program-level reporting, review and oversight of relevant capacity grant programs.
NIFA Reporting System	Consolidates the Plan of Work functionality into a new integrated system and will consolidate REEport functions in phases. The integrated system also adds new business functionality to allow Extension, capacity-funded programs to be registered with and reported to NIFA.
Research, Education, and Economics Information System (REEIS)	Provides information on NIFA's research, education, and extension programs as well as those of other USDA partner organizations.
Research, Extension, and Education Project Online Reporting Tool (REEport)	Collects technical and financial data on NIFA-funded grants and projects that allows grantees to report significant accomplishments and impacts of their research, extension, and education work.
RFA Tracker (RFA)	SharePoint application which provides for authoring, editing, and approval workflows and tracking of Request for Applications.

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?

The following three citations form the authority for NIFA to process and store this information:

- [Payment Integrity Information Act of 2019: 2 CFR 200.206](#)
- [Federal Funding Accountability and Transparency Act: 2 CFR 200.209](#)
- [2 CFR 200 Appendix I Part D: 2 CFR 200 Appendix I Part D](#)

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

Yes

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

N/A – GMRS is not a system of records.

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

N/A

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? 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.

Identifying Numbers:

- Taxpayer identification number
- Business taxpayer identification number (sole proprietor)
- Business mobile number (sole proprietor)

Biographical Information:

- Name (including nicknames)
- Race
- Business mailing address (sole proprietor)
- Business phone or fax number (sole proprietor)
- ZIP codes
- Business email address
- Resume or curriculum vitae

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

Grant program and funding information is entered, validated, and maintained by NIFA personnel. Grant applications are received from the Grants.gov system, which is operated and maintained by HHS. Those grant applications are submitted only by those individuals and organizations deemed as eligible in the various requests for applications (RFAs) published by NIFA. Additional information on grantees is obtained from SAM.gov, which is operated and maintained by GSA. Any individual or organization receiving payments from the federal government must maintain information within SAM.gov to be eligible to receive payments.

Grant applications, which are submitted via Grants.gov is the primary source for EIN/TIN, and Sam.gov is the source for verifying EIN/TIN that enters Grants Management and Reporting System. Grant applications containing EIN/TIN are received from Grants.gov via a system-to-system feed. EIN/TIN from Sam.gov is periodically updated in GMRS via a system to-system feed.

How is the information collected?

EIN/TIN is not collected directly from grant seekers, but that information is shared from HHS Grants.gov and GSA SAM.gov. Each of those systems is directly responsible for the collection of all EIN/TIN data contained within NIFA GMRS.

The information reaches GMRS in two ways. First, grant applications, submitted via Grants.gov, are received by GMRS via a system-to-system feed between GMRS and Grants.gov. Secondly, EIN/TIN, coming from SAM.gov to GMRS, is transferred in a system-to-system feed that is periodically refreshed.

Collection of EIN/TIN actually occurs within Grants.gov and SAM.gov, and that information is shared with NIFA GMRS.

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

No

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

EIN/TIN, as transferred from the grant application, is verified against the SAM.gov record of EIN/TIN for potential awardees.

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 through the use of third-party websites?

N/A

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk

- Unauthorized access to the PII (EIN/TIN) in GMRS

Mitigation

- The mitigation to this risk is only having authorized personnel to access this information through permissions granted in the system.
- EIN/TIN is encrypted whenever that data is in motion and is also encrypted when at rest (where it is stored within GMRS).
- EIN/TIN is only decrypted for authorized personnel to view within GMRS.
- At no time does a decrypted EIN or TIN appear on a report.

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?

Information is required to complete the authorization of funds by NIFA Office of Grants and Financial Management. This authorization process obligates the funds and makes them available for grantees to draw down.

EIN/TIN is used to identify potential and actual grantees for award, funds authorization, and funds transfer processes. EIN/TIN is also used in initialization of ASAP accounts used in funds transfer and drawdown. EIN/TIN is also used in verification of eligibility of a payee to receive payments from the US Federal Government through use of the DoNotPay system. ASAP and DoNotPay systems are hosted by the Department of Treasury.

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

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

Mitigation

- EIN/TIN, as received in GMRS from Grants.gov, and from SAM.gov is fully encrypted via SSL while in motion and is also encrypted when at rest (stored in the database).
- Only authorized personnel can access the data for specific use in award management and fund management processes.

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?

As described in section 1.4 above, NIFA GMRS does not collect information from individuals or institutional grant seekers. The data is shared from both HHS Grants.gov and GSA SAM.gov, which are the systems that govern the actual data collection. Hence, it is the policies and procedures of those two systems that provide primary notice. NIFA Requests For Applications (RFAs) also indicate to grant seekers that this information is required.

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

By applying for NIFA grant opportunities, applicants do agree and consent to use of information for purposes of verifying payment eligibility and facilitating authorization and transfer of funds. However, it is HHS Grants.gov and GSA SAM.gov that would handle gaining consent for particular uses of data.

Privacy Impact Analysis: Related to notice.

Privacy Risk

- Applicants are not aware of the purpose information is collected.

Mitigation

- Individuals and organizations applying for grants are aware of the data requirements for each application as detailed in the RFA for each funding opportunity.
- By the act of submitting a grant application, individuals and organizations are indicating awareness of the limited data being collected.
- Again, it is HHS Grants.gov and GSA Sam.gov that bear primary responsibility for notifying grant seekers of the risks involved and the relevant mitigations.
- NIFA GMRS does safeguard the data by always handling it in a secure manner and establishing controls to prevent unauthorized use of EIN/TIN.

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?

EIN/TIN, along with other information for grants must be retained for 15 years following cut-off. Cut-off is defined as the end of the fiscal year in which a grant is fully closed out.

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.

The National Institute of Food and Agriculture (NIFA) does maintain NARA-approved records control schedules. All schedules are listed under RG-0540: National Institute of Food and Agriculture (formerly Cooperative State Research, Education, and Extension Service).

Privacy Impact Analysis: Related to retention of information.

Privacy Risk

- The limited PII data retained in GMRS carries data potential risks of unauthorized access, unauthorized disclosure, or illegal use of the data.

Mitigation

- Data is hosted at USDA/DISC which follows USDA federal agency requirements for data protection and is accredited by FedRAMP.
- PII being maintained is encrypted when in motion and is also encrypted when at rest (stored in the database).
- Only authorized personnel can access PII data, and only for specific use in award management and fund management processes.
- **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?

Information is not shared within USDA.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk

N/A

Mitigation

N/A

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?

Data in GMRS is shared with US Treasury/Fiscal Service only as required for use in Treasury ASAP and Treasury DoNotPay systems. Eligibility of grantees to receive payments and authorization/transfer of funds cannot be completed without EIN/TIN. Meeting the process requirements of using ASAP for funds transfer and DoNotPay for eligibility are the reasons that EIN/TIN is collected from HHS Grants.gov and GSA SAM.gov.

Encrypted values for EIN/TIN are decrypted securely and transmitted only over encrypted and secure channels using system-to-system APIs or manually entered in Treasury ASAP and Treasury DoNotPay systems. At that point, it is the controls and policies put in place for Treasury systems that continue to safeguard privacy information.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk

- Information transfer is not secure and can be stolen en-route.

Mitigation

- Sharing of this type of sensitive information is routine in interfacing with Treasury/Fiscal Service systems.
- The transfer is governed by an ISA with Treasury/Fiscal Service, and NIFA has followed all Fiscal Service direction in enabling and securing information feeds.

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?

Grant applications are submitted to NIFA via Grants.gov, and applicants have the ability to gain access to submissions on that system. EIN/TIN is transferred from SAM.gov, where applicants and grantees have the ability to access and edit their own information.

What are the procedures for correcting inaccurate or erroneous information?

Applicants may edit and correct and resubmit grant applications prior to submission deadlines as specified in the RFA for each funding opportunity. Applicants and grantees may edit their data at SAM.gov at any time to make corrections or changes.

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

For grant application revision, correction, and resubmission Grants.gov maintains online help resources to submit changed and corrected applications. Similarly, SAM.gov has online help resources to update and correct data including EIN/TIN.

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

The Department of Health and Human Services for Grants.gov, and the General Administrative Administration for SAM.gov each provides a procedure of alternatives to individuals regarding redress and alternatives.

Privacy Impact Analysis: Related to redress.

Privacy Risk

- **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.

Mitigation

- **Establish Clear Procedures:** 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?

GMRS has multiple layers of cyber defense and strict layered access control procedures. EIN/TIN are encrypted when stored in our databases

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

GMRS system components use documented application permissions and some role-based access methods to control access to system users.

How does the program review and approve information sharing requirements?

NIFA Formal review and approval process is in place for the respective sharing agreements

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

The Annual Information Security Training provides the training necessary and sufficient for users to interact with this system and understand how to handle information securely.