Privacy Impact Assessment

NIFA Grants Management and Reporting System

- Version: 1.7
- Date: June 2023
- Prepared for: USDA NIFA

United States Department
of Agriculture

Privacy Impact Assessment for the

Grants Management and Reporting System (GMRS)

National Institute of Food and Agriculture (NIFA)

June 2023

Contact Point

Pratima Boyapati
Deputy Assistant Chief Information Officer (DACIO)
202-701-3529

Reviewing Official

Renato Chan
Assistant CISO (ACISO)
202-720-4068

Abstract

The Cooperative Research, Education, and Extension, Management System (C-REEMS) is a component of Grants Management and Reporting System (GMRS). 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. The Privacy Impact Assessment (PIA) is being conducted as the Privacy Threshold Assessment (PTA) was conducted on the GMRS and was found to have PII in the form of having EIN/TIN in C-REEMS and thus this assessment is being completed.

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 disbursal; 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

Applications	Description
Award Document Repository (ADR)	ADR is NIFA's official electronic grant records repository for non-capacity grant programs. ADR provides functionality to perform records management activities including storage, uploading, search and retrieval and disposition of records.

Applications	Description
Aurea ListManager (ALM)	Lyris 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 Lyris 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 ticket management capabilities to business units.
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)	Provides data and reports on NIFA's research, education and extension activities supported by NIFA, state, and other federal agencies. Provides the capability to search, retrieve and display results using URLs that can be leveraged on NIFA's website and other communication channels.
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.

Applications	Description
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.
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 project, financial and budget information on the agency's programs.
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.

Applications	Description
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 1.0 Characterization of the Information

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

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

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. EIN/TIN (Employer ID Number/Taxpayer ID Number) of awardees is required in order to complete authorization of funds for each award. It has been determined that EIN/TIN, when added to contact information on awardees, constitutes PII.

1.2 What are the sources of the information in the system?

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.

1.3 Why is the information being collected, used, disseminated, or maintained?

EIN/TIN 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 drawdown.

1.4 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. Secondarily, 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.

1.5 How will the information be checked for accuracy?

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

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The following three citations form the authority for NIFA to collect this information:

- 2 CFR 200.206 (https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-C/section-200.206)
- 2 CFR 200.209 (https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-C/section-200.209)
- 2 CFR 200 Appendix I Part D (https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/appendix-Appendix%20I%20to%20Part%20200)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Unauthorized access to the PII (EIN/TIN) in C-REEMS. 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 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

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.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Only C-REEMS and Treasury DoNotPay application functions are used to view data. Only clearance of control gates for award of federal grants, authorization of funds is a direct output of uses of EIN/TIN.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

No commercial or publicly available data is used in conjunction with EIN/TIN.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

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 3.0 Retention

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

3.1 How long is information retained?

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.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

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).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

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

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.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

EIN/TIN is not shared within USDA.

4.2 How is the information transmitted or disclosed?

N/A

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

N/A

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

EIN/TIN data in GMRS is shared with US Treasury/Fiscal Service only as required for use in Treasury ASAP and Treasury DoNotPay systems.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, sharing with Treasury/Fiscal Service is compatible with the original collection. 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 reason that EIN/TIN is collected from HHS Grants.gov and GSA SAM.gov.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

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.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

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 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes, the GMRS requires a SORN. The Agency is currently working on publishing the SORN.

6.2 Was notice provided to the individual prior to collection of information?

As described in section 1.4 above, NIFA GMRS does not collect EIN/TIN 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.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

No, if grant seekers wish to be eligible to receive grant payments, the information is considered mandatory.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

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

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

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 to NIFA 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 7.0 Access, Redress and Correction

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

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The Department of Health and Human Services and the General Services Administration as the collectors of information each should provide this assessment of the risks associated with redress and mitigation plans for those risks.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

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

8.2 Will Department contractors have access to the system?

Contractors to NIFA are often granted access to GMRS, only as authorized by NIFA management.

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

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.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, we have a current ATO.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system contains access logs, secure database storage, and network/application-level security measures that have been established to identify and prevent any misuse of data. Business process controls have also been established by the NIFA Office of Grant and Financial Management to identify and prevent any fraudulent activity and data misuse.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted

on the system, what privacy risks were identified and how do the security controls mitigate them?

The principal privacy risks are the misuse of privacy data and unauthorized access to privacy data. The methods of mitigation include the maintenance of sufficient access controls, annual information security training, and periodic security reviews conducted by USDA REE and USDA OCIO.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Grant applications are retrieved from Grant.gov using the Grants Application Connector (GAC) application component. GAC pulls grant applications which contain EIN/TIN from Grants.gov via a secure API provided by HHS Grants.gov for use in C-REEMS. CDS (Communication and Distribution System) is the application component that picks up the grant application from GAC and loads selected data from the grant application into C-REEMS. C-REEMS is the core grants management application within GMRS. GAC and CDS are Java browser-based applications served by a RedHat JBoss EAP cluster and running on RHEL. C-REEMS is an Oracle Forms and Reports Application served by Oracle WebLogic and running on RHEL. All servers are hosted at the USDA EDC at DISC in Kansas City. GAC, CDS and C-REEMS are custom-built applications that have been built and maintained by NIFA.

Data that includes EIN/TIN is imported from GSA SAM.gov on a regular schedule using a scheduled and scripted secure FTP service that is provided by GSA. The scheduled job runs on a secure RHEL server that is hosted at the USDA EDC at DISC in Kansas City.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The privacy concerns surrounding the technology used by all GMRS application components are typical of any browser-based information system. Security controls have been established over many years, and those controls are regularly and periodically reviewed and adjusted to keep pace with accepted good security practices.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of

Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

N/A

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

N/A

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A