Privacy Impact Assessment
Emergency Management Response Services 2.0

Technology, Planning, Architecture, & E-Government

- Version: 1.9
- Date: March 23 2023
- Prepared for: Marketing and Regulatory Programs

Privacy Impact Assessment for the

Emergency Management Response Services 2.0 (EMRS2)

March 2023

Contact Point
Jonathan Zack, DVM
APHIS Veterinary Services
United States Department of Agriculture
(301) 851-3460

Reviewing Official
Tonya Woods
Director, Freedom of Information and Privacy Act Staff
United States Department of Agriculture
(301) 734-8296

Abstract

The Emergency Management Response Services 2.0 (EMRS2) is a Major Application used by the APHIS Veterinary Services (VS) to manage and investigate animal disease outbreaks in the United States. The system is used by Federal, State, Tribal, and local animal health officials and human health officials. This Privacy Impact Assessment (PIA) is being completed following the Privacy Threshold Analysis (PTA) conclusion requiring a PIA for EMRS2 to meet federal privacy compliance requirements.

Overview

The EMRS2 is an incident management data collection system is utilized by Veterinary Services to manage and investigate animal disease outbreaks and instances of foreign animal disease (FAD) in the United States. The EMRS2 business requirement has three main process domains: Investigation management, Lab Submission management, and Resource management.

EMRS2 is custom built within the Microsoft 365 platform and is accessed by approved users via Microsoft Internet Explorer. Primary users of EMRS2 are Federal and State veterinary medical officers, animal health technicians, and various disease specialists and epidemiologists from APHIS and from State cooperators.

There are two extensions to EMRS2 also in use which serve as alternate user interfaces but enforce all applicable security thru the Dynamics API:

1) *Gateway*
2) *EMRS2GO*

The Gateway allows producers to request and manage movement permits. Users do not receive EMRS2 accounts and cannot interact directly.

EMRS2GO is a Windows Presentation Foundation application that runs on the users' laptop. It exposes the Incident Contact Reports (ICR) and other forms to the user in an effort to minimize their entry errors. The EMRS2GO application, like the Gateway, leverages the Dynamics API.

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 collects, uses and maintains information such as:

Owner or operator of the premises where the animals subject to investigation are located; the system includes the following information, such as, but not limited to, the name; address (including city, county, State, postal code, and latitude/longitude coordinates); premises identification number; and telephone number.

Referring contact information, which includes name and telephone number.

Case coordinator of the premises investigation; the system includes name, telephone number, and email address.

APHIS employees; the system includes the following information, such as, but not limited to the name; agency, program, and group; current duty assignment; encrypted employee identification number; grade, series, and step; duty city and State; home address, including latitude/longitude coordinates; home telephone number; home email address; emergency contact information; work and field addresses, email addresses and telephone numbers; and supervisor contact information.

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

The sources of the information are customers defined as, owner or operator of the premises where the animal(s) subject to investigation are located; and from APHIS VS employees, referring contact, and case coordinator. Such information may be supplemented by other sources of information such as, an address-validation database, by APHIS personnel during an on-site investigation, by State and Tribal veterinarian offices and State laboratories, or by APHIS' National Veterinary Services Laboratories. Information may also be sourced from the Financial Management Modernization Incentive for payment status. Employee information is obtained primarily from the employee. Additionally, employee information may be obtained from the U.S. Department of Agriculture's (USDA's) National Finance Center, AgLearn database, and Federal Occupational Health, U.S. Department of Health and Human Services.

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

Data is used by VS to manage and investigate animal disease outbreaks in the United States. This information is required to process numerous documents such as those needed for indemnity to owners/growers, reimbursement for cleaning and disinfection, and record keeping for surveillance, testing. The system is used by Federal, State, Tribal, and local animal health officials (and human health officials) for:

- Routine reporting of Foreign Animal Disease (FAD) investigations
- Surveillance and control programs
- State-specific disease outbreaks
- National animal health emergency responses

1.4 How is the information collected?

Information is provided to APHIS, as well as State and Tribal officials to enter this information into the main EMRS2 application, or the Gateway (by producers/owners and growers) and EMRS2GO extensions when appropriate. State and local Veterinary Officers and various disease program laboratories provide data for use in EMRS2, depending upon the geographic extent of the animal disease outbreak, and dependent upon if an appropriate data sharing Memorandum of Understanding (MOU) is in place with USDA. The mapping module occasionally utilizes public data from the U.S. Geological Survey and other Federal resources available to the public.

1.5 How will the information be checked for accuracy?

Authorized federal, state, or EMRS2 personnel that collect and enter the data are responsible for the review and accuracy of the data. Information is obtained from either a customer or an employee and is often supplemented during an investigation by on-site visits, USPS database, or other address-validation databases. There are also limited data entry constraints to ensure entry completeness. APHIS employees also have access to the EMRS2 Administrative module where they may edit and maintain their own employee profiles. EMRS2 updates Employee Profiles via records in the Emergency Qualification System (EQS) that is shared using a flat file each quarter. When an employee profile changes, EMRS2 receives the updated information via the next scheduled EQS file share. (EQS gets their data from the National Finance Center (NFC) bi-weekly).

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

APHIS is an emergency response organization whose mission is to protect the health and value of U.S. agricultural, natural and other resources.

The Animal Health Protection Act (AHPA) (7 U.S.C.8301 et seq.) provides the authority for the Secretary to prevent, detect, control, and eradicate diseases, and pests of birds and other livestock to protect animal health, the health and welfare of people, economic interests of livestock and related industries, the environment, and interstate and foreign commerce in birds, other livestock, and other articles. EMRS2 is the system used to act on this authority.

Any additional authority comes from the specific state under which investigation is occurring.

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, inaccurate data and unauthorized use are privacy risks associated with the amount and type of data in EMRS2.

Unauthorized access risks are mitigated by the following means:

- Users accessing EMRS 2 must successfully authenticate using their e-Authentication PIV or e-Authentication username/password credential and be authorized with specific EMRS role(s).
- The application limits access to relevant information and prevents access to unauthorized information.
- Devices running the EMRS2GO extension must have a government approved encryption in place or the application will not run.
- Users of EMRS2GO must have an authorized account in the EMRS2 web application.

Data is secured by means of encryption and access control. Access is controlled by:

- User ID and password or PIV card
- e-Authentication
- Access Control list
- Read and write authorization permissions that are specific to individual EMRS2 electronic forms
- Microsoft Dynamics 365 role-based access control.

The accuracy of the customer information is confirmed with the customer prior to submission into the EMRS2. This helps to mitigate the risk of inaccurate information at the point of collection.

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.

Data is used by VS to manage and investigate animal disease outbreaks in the United States. The system is used by Federal, State, Tribal, and local animal health officials (and human health officials) for:

- Routine reporting of Foreign Animal Disease (FAD) investigations
- Animal disease surveillance and control programs
- State-specific animal disease outbreaks
- National animal health emergency responses

When other Federal and State emergency response agencies assist USDA with an emergency disease outbreak, they may be allowed limited access to the data in

EMRS2. The access will depend upon the MOU in place and the need to know of the other agency. Data will be used for:

- Routine reporting of FAD investigations
- Surveillance and control programs
- State-specific disease outbreaks
- National animal health emergency responses

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

Microsoft Dynamics 365 includes customizations to allow users to visualize and understand data using GIS mapping to support situational awareness needs.

Dynamics 365 also includes features to allow users to analyze data in various ways. The most basic analysis tool is the view. Users may customize views to display data sorted by specific field and display only the data in selected fields. Users may only view the data to which they have access based on their role, as defined in Dynamics 365. Users may also create charts and graphs to show trends and statistical information. Users can create dashboards to display information that is customized to their needs.

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

EMRS2 uses Bing Maps for imagery only and utilizes no other Bing Map services. These maps are needed to assess the geographical location of infected premises and at-risk premises within the control area and/or surveillance zone. Field responders utilize geographical coordinates to conduct surveillance activities in the affected area.

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.

Data is secured by means of encryption and access control. Access is controlled by:

- User ID and password or PIV card
- e-Authentication
- Access Control list
- Read and write authorization permissions that are specific to individual EMRS2 electronic forms
- Microsoft Dynamics 365 role-based access control.

The VS management team and National Preparedness and Incident Coordination Center management will determine when data needs to be consolidated and ensure date is protected from unauthorized access.

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?

As of today, records are retained permanently in accordance with unscheduled records management policy. Once scheduled and approved by NARA, all EMRS records will be retained for 50 years.

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

APHIS VS has developed record retention schedules, but until they are approved by NARA, electronic systems are classified as permanent in accordance with unscheduled records management policy.

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

Risks associated with data retention are minimal and include the possibility of the data being accessed by unauthorized personnel. EMRS2 uses role-based access to mitigate this risk. The VS Leadership team and National Preparedness and Incident Coordination Center staff, State Veterinarians and EMRS2 team members and authorized users are all responsible for protecting the privacy rights of the customers and employees affected by the interface. The login interface reminds users of their responsibility every time they log in.

On mobile devices the mitigation above holds true: the EMRS2GO extension uses the user's EMRS2 account for authentication and authorization, such that they cannot gain any further access than they already have. Additionally, the mobile extension will only run on devices with an approved encryption and there are controls on the concurrency of the data related to last access of the application such that if the application is not used for a government-determined period, the application will be forced to synchronize, and in the event the EMRS account is no longer valid the sync will not return data and existing reference data will be wiped.

Disclosure or disposal of the data poses additional risks to this data, and this is mitigated by ensuring the implementation of technical controls such as auditing, access control and system communications; the implementation of operational controls like configuration management, contingency planning, system and security integrity, and the implementation of management controls such as annual risk assessments, planning and security assessment and authorization, are in place and operating as expected. These controls are explained in NIST Special Publication 800-53.

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?

EMRS2 does not share data with any internal organizations outside the parameters of standard user access.

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?

(1) To certain Federal, State, and Tribal animal health officials to identify premises before an event to allow for faster response, monitor the status of an animal disease investigation, document actions taken relating to an animal disease investigation, track the status of animals susceptible to foreign animal diseases, determine the costs of an animal disease investigation, monitor the use and availability of assets and personnel relating to animal disease investigations, or perform epidemiological and geospatial analyses of such investigations;

(2) To Federal, State, and Tribal animal health officials within the system to obtain feedback regarding the EMRS system and emergency preparedness guidelines, and to educate and involve them in program development, program requirements, and standards of conduct;

(3) When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program, statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, Tribal, local, or other public authority

responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity;

(4) To the Department of Justice when: (a) USDA or any component thereof; or (b) any employee of USDA in his or her official capacity, where the Department of Justice has agreed to represent the employee; or (c) the United States Government, is a party to litigation or has an interest in such litigation, and USDA determines that the records are relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by USDA to be for a purpose that is compatible with the purpose for which USDA collected the records;

(5) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when USDA or other Agency representing USDA determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding; ;

(6) To appropriate agencies, entities, and persons when: (a) USDA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) USDA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(7) To another Federal agency or Federal entity, when information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the agency (including its information systems, programs, and operations), the Federal Government, or national security;

(8) To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the USDA, when necessary to accomplish an agency function related to this system of records;);

(9) To Congressional office staff in response to an inquiry from that Congressional office made at the written request of the individual about whom the record pertains; and

(10) APHIS may disclose information in this system of records to the National Archives and Records Administration or to the General Services Administration for records management inspections being conducted under 44 U.S.C. 2904 and 2906.

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. The sharing of personally identifiable information outside the Department is compatible with the original collection.

System of Records Notice APHIS-11 Emergency Management Response System describes the applicable routine use that covers this external sharing of personally identifiable information.

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

Information shared outside the Department falls within the disclosures outlined in section 5.1. The data are extracted per the requested parameters and is then transmitted to the requesting internal point of contact using secure protocols and connections. The actual sharing to the external source is done by the USDA APHIS Privacy Act Office in the Legislative and Public Affairs (LPA) Branch.

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

Information shared outside the Department falls within the disclosures outlined in section 5.1. The data is extracted or transferred per specific parameters and is then transmitted to the requesting partner organizational system using secure protocols and connections. Where the external sharing is the result of a Freedom of Information Act request, the actual sharing to the external source is done by the USDA APHIS Privacy Act Office in the Legislative and Public Affairs (LPA) Branch.

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

Yes.

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

Yes. There is no penalty at the federal level if user refuses to provide information. Any consequences are enforced at the state level.

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

Yes. Information is collected only for specified circumstances or investigation, and this information is not utilized for any other purpose other than for those collected. Use of data is limited to the use for which it was collected and EMRS2 staff does not release information unless there is an overriding reason as stated under 5.1. Individuals do not access records in EMRS2. Freedom of Information Act requests must be in writing and should be submitted to the APHIS Privacy Act Officer, 4700 River Road Unit 50, Riverdale, MD 20737; or by facsimile (301) 734-5941; or by email APHISPrivacy@usda.gov. In accordance with 7 CFR 1.112 (Procedures for requests pertaining to individual records in a record system), the request must include the full name of the individual making the request; the name of the system of records; and preference of inspection, in person or by mail. In accordance with 7 CFR 1.113, prior to inspection of the records, the requester shall present sufficient identification to establish that the requester is the individual to whom the records pertain. In addition, if an individual submitting a request for access wishes to be supplied with copies of the records by mail, the requester must include with his or her request sufficient data for the agency to verify the requester's identity.

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

Notice is provided via the publicly available System of Record Notice, the Privacy Impact Assessment (this document) and Memorandum of Understanding with other organizations. No information is collected without the awareness of an individual. Permission is requested of the premise or animal owner to collect information. In the case of a disease outbreak, the federal government has jurisdiction/authority to collect animal health information relevant to an infected premise or premise in a control area. The Privacy Act Notice is posted on the EMRS2 Home Page as a point of reference and additional notification to the individuals.

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?

Individuals do not access records in EMRS2. Freedom of Information Act requests must be in writing and should be submitted to the APHIS Privacy Act Officer, 4700 River Road Unit 50, Riverdale, MD 20737; or by facsimile (301) 734-5941; or by email APHISPrivacy@usda.gov. In accordance with 7 CFR 1.112 (Procedures for requests pertaining to individual records in a record system), the request must include

the full name of the individual making the request; the name of the system of records; and preference of inspection, in person or by mail. In accordance with 7 CFR 1.113, prior to inspection of the records, the requester shall present sufficient identification to establish that the requester is the individual to whom the records pertain. In addition, if an individual submitting a request for access wishes to be supplied with copies of the records by mail, the requester must include with his or her request sufficient data for the agency to verify the requester's identity.

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

Individuals seeking to contest or amend records maintained in this system of records must direct their request to the address indicated above in the "RECORD ACCESS PROCEDURES" paragraph and must follow the procedures set forth in 7 CFR 1.116 (Request for correction or amendment to record). All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

If an individual experiences a change in contact information, they may reach out to their state or federal point of contact and request a correction. The state or federal contact, may then correct the information in the EMRS2 or elevate the request directly to the VS Emergency Management Coordinator.

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

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the "RECORD ACCESS PROCEDURES" paragraph above.

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

N/A. The formal redress process is described under section 7.1 above.

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

No privacy risk has been identified.

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?

Access to EMRS2 is based on the need to conduct business within USDA and is approved by an authorized APHIS VS official. Criteria, procedures, and controls are documented. Access must be requested in writing and approved by the supervisor and an EMRS2 account manager.

8.2 Will Department contractors have access to the system?

No

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

All USDA APHIS VS employees are required to complete annual Information Security Awareness Training and sign Rules of Behavior. This general training allows organizational users with access to personally identifiable information to receive privacy-related training.

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

Yes. The USDA APHIS VS EMRS2 received a renewed Authority to Operate (ATO) that expires on May 8, 2023.

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

Some of the technical safeguards for EMRS 2.0 using Dynamics CRM is a security model that includes auditing, role-based views, field-level security, and division of security. This means changes to records are tracked. Even the audit history on individual record and/or audit history summary is also tightly controlled with separate security settings to protect the integrity of the log. The security model only provides users with access only to the appropriate levels of information based on their role(s). Furthermore, views and field-level are role-based as well; preventing users from seeing, accessing, and/or making changes to individual fields or records they do not have access to. Finally, access control is a combination of eAuthentication (user credential and authentication) and authorization (EMRS2 roles).

The EMRS2GO mobile Application uses 3 controls to protect downloaded data.

- Assures the hard drive has Bit Locker or a similar data encryption application or the app will shut down before a download of any data.
- After 30 days, if the reference data have not been uploaded to the EMRS system, EMRS2Go performs a full data upload regardless of the options the user has selected.

- After 60 days, if the reference data have not been uploaded, EMRS2Go deletes the local repository and performs a full data upload regardless of the option the user selected. If user no longer has access to EMRS, no data is downloaded after local data is deleted.

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?

As to technical safeguards:

- The EMRS2 is continuously monitored to ensure changes to the data is logged and reviewed. Auditing is performed to also alert the database administrators to privileged action taken against the database objects. The logs are correlated and saved at an Enterprise level to aid forensic investigation if the need arises.
- Access control technical measures are in place and operating to ensure only users with approval can access the data, and the concept of least privileged is enforced to ensure only the minimum access and privileges are granted to enable users to perform the job function. User access is audited on a continual basis.
- Operational technical safeguards to prevent data misuse begin with access control. EMRS2 employs TLS encryption to protect data during transmission and enforces multifactor authentication for user access. Password controls, procedures, responsibilities, and policies follow USDA departmental standards. APHIS employees must use LincPass to access their computer and the APHIS network, including the VPN. There is no action that can be performed within the EMRS2 without identification and authentication.
- At the USDA and APHIS Enterprise level, intrusion detection and intrusion prevention, firewalls and antivirus measures are employed on a continuous basis.

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?

Animal Health/Incident Response Management.

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

This application does not employ technology which may raise privacy concerns.

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?

EMRS2 uses Bing Maps for imagery only and utilizes no other Bing Map services. These maps are needed to assess the geographical location of infected premises and at-risk premises within the control area and/or surveillance zone. Field responders utilize geographical coordinates to conduct surveillance activities in the affected area.

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

EMRS2 does not receive any personally identifiable information from third party websites or applications.

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

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

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

EMRS2 does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Responsible Officials

JONATHAN ZACK
Digitally signed by JONATHAN ZACK
Date: 2023.11.22 08:45:29 -05'00'

Jonathan T. Zack
EMRS2 System Owner
United States Department of Agriculture

Approval Signature

Janelle Jordan
Digitally signed by Janelle Jordan
Date: 2023.12.01 13:44:21 -05'00'

Janelle J. Jordan
APHIS Privacy Act Officer
United States Department of Agriculture

ANGELA COLE
Digitally signed by ANGELA COLE
Date: 2023.12.01 14:04:00 -05'00'

Angela Cole
Chief Privacy Officer/Deputy Assistant Chief Information Security Officer
Marketing and Regulatory Programs
United States Department of Agriculture