Privacy Impact Assessment

Technology, Planning, Architecture, & E-Government

- Version: 1.8
- Date: December 2020
- Prepared for: USDA APHIS VS
  Emergency Response Management
  Services 2.0 (EMRS2)

United States Department of Agriculture

Privacy Impact Assessment for the

Emergency Management Response Services 2.0 (EMRS2)

December 2020

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 used 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. EMRS2 also utilizes the BING mapping Web service graphical user interface for easy visualization of work areas. 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. In an animal disease emergency, VS could potentially enlist the assistance of accredited private veterinary practitioners who assist with disease exclusion, detection, and control.

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. It is a web application built on the Dynamics 365 API using level 1 authentication. Users do not receive EMRS2 accounts and cannot interact directly. It reduces the cost of managing permits by making the process more efficient thru a single secure data entry point instead of reentry of volume requests received thru multiple methods by employees into EMRS and maintains communications within the system which in the past had to be handled primarily through email.

EMRS2GO is a Windows Presentation Foundation application that runs on the users' laptop. It exposes the Incident Contact Reports (ICR) and other forms, such as Tasks, 214 Daily Reports, Euthanasia and Disposal (E & D) and Clean and Disinfect (C & D), to the user in an effort to minimize their entry errors and training needs. Many users have no further need to interact directly within the EMRS2 application and EMRS2GO allows only the functionality needed to perform these tasks. It uses a three tiered approach to protect downloaded data when the application is started. These include the requirement for hard drive encryption, the monitoring of downloads and the wiping of any downloaded data from the user's laptop once access is no longer needed to the EMRS2 system. The EMRS2GO application, like the Gateway, leverages the Dynamics API. Authorized users must have a valid EMRS2 account, as well as a level 2 USDA eAuthentication account.

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?

Information includes, but is not limited to, name; address (including city), county, state, postal code, latitude/longitude coordinates; premises identification number; and telephone number. The EMRS2 may include, but is not limited to, name and telephone number of the person(s) who provided the initial report concerning the premises, and the name, telephone number, and email address of the person responsible for the investigation of the premises. EMRS2 also contains information about APHIS employees who may be deployed as members of Incident Command System (ICS) teams and their position assignment.

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

Owner or operator of the premises where the animal(s) subject to investigation are located and APHIS VS employees, referring contact, and case coordinator.

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. 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?

State and local Veterinary Officers and various disease program laboratories provide data for use in EMRS2, depending upon the geographic extent of the particular 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.

Information is entered through the main EMRS2 application, or the Gateway and EMRS2GO extensions when appropriate.

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

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

Privacy rights of the customer and employees will be protected by USDA, APHIS and VS management.

- 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.

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
- In the cloud controlled by servers also existing in the cloud
- 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 or use based on user roles as well.

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.

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
- In the cloud controlled by servers also existing in the cloud
- 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?

Routine FAD data from EMRS2 is expected to be retained on the server for an indefinite time. Employee data is maintained as long as employee is employed and may be maintained for up to five years after employment ceases in case employee is re-employed during emergencies. After an animal outbreak, data is retained a minimal of twenty years for an active record, and ten years for inactive records.

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

No. Records retention in this application has not specifically been approved by NARA. Approval was requested and is being tracked under POA&M ID 27667.

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 management 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.

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 shares data with any USDA organizations like Agricultural Research Service, Animal Care and Wildlife Services, in case of emergency disease outbreaks. Data is also shared with the new VS Data Integration Services system hosted on Palantir in the MRP AWS GSS to support management and mission-oriented decisions.

4.2 How is the information transmitted or disclosed?

The data will be retrieved (transmitted to user) through selection queries to:

- View Data
- Create reports
- Create maps of specific areas
- Server agent nightly data pulls

Data can be retrieved only by personnel who successfully authenticate using their e-Authentication PIV or e-authentication username/password credential and are authorized with specific EMRS role(s). If data is retrieved via the email client no record of data queried is kept, but individual must have user access and rights to access data. Data can be retrieved by a full text search or a defined search. The full text search allows any data matching the entered data element to be retrieved. In the Investigation module, defined search data can be retried by: Premises ID, Reference Control Number, Premises, Name, Incident Group, or Incident Site. In the Administration module, defined search data can be retrieved by: employee, property, fleet vehicle, ledger, last name, first name, employee ID, nickname, title, organization, or section.

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.

In emergency disease outbreak situations where internal agencies assist EMRS2 with management activities, there is a potential for information to be shared with unauthorized users. It is the intent of EMRS2 that the uses of information remain in accordance with the stated purpose and use of the original collection at all times. Steps will be taken to ensure that access to the information system is provided only to authorized users. Data will be used by USDA, Federal and State FADDs, the laboratories, and animal health officials to document, manage, and communicate activities and findings while conducting routine foreign animal disease investigations.

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

(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 their agents, grantees, experts, consultants, and other 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. Individuals providing information under this routine use are subject to the same Privacy Act requirements and limitation on disclosure as are applicable to USDA officers and employees;

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

(10) To the National Archives and Records Administration or other Federal Government agencies pursuant to 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.

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?

The data will be retrieved through selection queries to:

- View data
- Create reports
- Create maps of specific areas

Data can be retrieved only by personnel who successfully authenticate using their e-Authentication PIV or e-authentication username/password credential and are authorized with specific EMRS role(s). If data is retrieved, no record of data queried is kept but individual must have user access and rights to access data. Data will be retrieved thru views, reports, and queries to view data, create reports and create maps. Users must be authenticated and have role based access to data which is limited to a need to know basis to the users business unit (generally state level access). Data can be retrieved through searching the fields that have been enabled to be indexed and searchable, and would not include any fields the users does not have access to via field level security.

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

The uses of information are in accordance with the stated purpose and use of the original collection. Data will be used by VS Federal and State FADDs, the laboratories, and animal health officials to document, manage, and communicate activities and findings while conducting routine foreign animal disease investigations.

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. The EMRS2 notice is located at:
http://ww.ocio.usda.gov/APHIS-11Emergency_Management_Response_System(EMRS).txt

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 over-riding reason.

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.

Privacy Banner and MOU with other Organizations

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?

Any individual may obtain information from a record in the system that pertains to him or her. Request for hard copies of records should be in writing, and the request must contain the requesting individual’s name, address, name of system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the APHIS Privacy Act Officer, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address above. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

Individuals are notified of procedures at the point of data collection.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manger to the APHIS Privacy Act Officer, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

Once received by the VS the requests to correct information are treated as sensitive material in accordance with the formal redress methods. Any data used or furnished to others would need to be cleared through the Freedom of Information Act process.

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 Need-to-know and role-based access.

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 Security Training and a select group of individuals must also complete Privacy training.

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

The USDA APHIS VS EMRS2 received a renewed Authority to Operate (ATO) until May 10, 2020.

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

In accordance with FIP 199/200 Moderate Baseline Security Controls. 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 any events, such as create, modified, soft deletion, users, old and new values are audited at the field level. 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 synched, EMRS2Go performs a full sync regardless of the option the user selected.
- After 60 days, if the reference data have not been synched, EMRS2Go deletes the local repository and performs a full sync 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 <u>Privacy Impact Analysis</u>: 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 data will be retrieved through selection queries to:

- View data
- Create reports
- Create maps of specific areas

Data can be retrieved only by personnel who have logged in with their e-Authentication PIV or e-authentication username/password credential and have been authorized with specific EMRS role(s). If data is retrieved, no record of data queried is kept but individual must have user access and rights to access data. Data will be retrieved thru views, reports, and queries to view data, create reports and create maps. Users must be authenticated and have role based access to data which is limited to a need to know basis to the users business unit (generally state level access). Data can be retrieved through searching the fields that have been enabled to be indexed and searchable and would not include any fields the users do not have access to base upon field level security.

In addition, requiring encryption the following two controls referenced in previous section address data stored on the device:

- After 30 days, if the reference data have not been synched, EMRS2Go performs a full sync regardless of the option the user selected.
- After 60 days, if the reference data have not been synched, EMRS2Go deletes the local repository and performs a full sync regardless of the option the user selected. If user no longer has access to EMRS no data is downloaded after local data is deleted.

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?

Major Application – 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?

EMRS uses Bing Maps for imagery only and utilizes no other Bing Map services.

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?

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

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?

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

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

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

10.7 Who will have access to PII that becomes 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.

10.8 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?

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

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)?

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

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?

EMRS2 does not use web measurement and customization technology.

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.

EMRS2 does not collect or transmit any PII data from any third-party application.

Responsible Officials

Jonathan Zack, DVM

APHIS-VS

United States Department of Agriculture

Approval Signature

JONATHAN ZACK Digitally signed by JONATHAN ZACK
Date: 2020.12.14 17:19:34 -05'00'

Jonathan Zack, DVM
System Owner
United States Department of Agriculture

PRESTON GRIFFIN Digitally signed by PRESTON GRIFFIN
Date: 2020.12.30 08:38:59 -05'00'

Preston Griffin
MRP IT ISSPM
United States Department of Agriculture

JANELLE JORDAN Digitally signed by JANELLE JORDAN
Date: 2020.12.28 15:25:58 -05'00'

Tonya Woods
APHIS Privacy Officer
United States Department of Agriculture