

Supporting Statement – Part A
OMB Control Number – 0579-XXXX

Title: Center for Epidemiology and Animal Health (CEAH), National Animal Health Monitoring System (NAHMS)¹ Data Security Requirements for Accessing Confidential Data
Date Prepared: January 2025

Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection of information. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

This is a request for new ongoing information collection request. APHIS is asking the Office of Management and Budget (OMB) to approve this request for 3 years.

Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (44 U.S.C. 3583; hereafter referred to as the Evidence Act) mandates that the Director of the Office of Management and Budget (OMB) establish a standard application process (SAP) for requesting access to certain confidential data assets. While the adoption of the SAP is required for statistical agencies and units designated under the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA), it is recognized that other agencies and organizational units within the Executive Branch may benefit from the adoption of the SAP to accept applications for access to confidential data assets. The SAP is to be a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access confidential data assets held by a Federal statistical agency or unit for the purposes of developing evidence. This new process will be implemented while maintaining stringent controls to protect confidentiality and privacy, as required by law.

Data collected, accessed, or acquired by the Federal statistical agencies and units is vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. This evidence can benefit the stakeholders in the programs, the broader public, as well as policymakers and program managers at the local, State, Tribal, and National levels. The many benefits of access to data for evidence building notwithstanding, the U.S. Department of Agriculture's (USDA's), Animal and Plant Health Inspection Service's (APHIS'), National Animal Health Monitoring System (NAHMS) is required by law to maintain careful controls that allow it to minimize disclosure risk while protecting confidentiality and privacy. The fulfillment of NAHMS' data security requirements places a degree of burden on the public, which is outlined further in this justification.

In late 2022, the National Center for Science and Engineering Statistics (NCSES) within the National Science Foundation (NSF), in its role as the SAP Project Management Office (PMO),

¹ The National Animal Health Monitoring System is responsible for collecting national data on animal health and productivity from voluntary participants.

published a 60-day Federal Register Notice ([87 FR 53793](#)) and 30-day Federal Register Notice ([87 FR 66754](#)) announcing plans to collect information through the SAP Portal. This collection request was submitted to the Office of Management and Budget as a Common Form in late 2022; their OMB control number for SAP Portal information collection is 3145-0271 and the expiration date is December 31, 2025.

With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied are working with the SAP (PMO) and with OMB to implement the SAP. The SAP Portal is a single web-based common application designed to collect information from individuals requesting access to confidential data assets from Federal statistical agencies and units. The objective of the SAP Portal is to broaden access to confidential data for the purposes of evidence building and reduce the burden of applying for confidential data on or for the American public or public researchers.

Once an application for confidential data is approved through the SAP Portal, NAHMS will collect information to fulfill its data security requirements. This is a required step before providing the individual with access to confidential microdata for the purpose of evidence building. NAHMS' data security agreements and other paperwork, along with the corresponding security protocols, allow NAHMS to maintain careful controls on confidentiality and privacy, as required by law. This collection will occur outside of the SAP Portal. On August 19, 2024, APHIS–NAHMS published a 60-day Federal Register Notice (89 FR 67058) announcing plans for this collection.

The paragraphs below outline the SAP Policy, the steps to complete an application through the SAP Portal, and the process for agencies, such as APHIS, to collect information fulfilling their data security requirements. After accessing the SAP Portal and discovering confidential data assets, an applicant must submit an application via the SAP Portal for review. Upon receiving a positive determination, an applicant will be required to complete training and security requirements prior to accessing confidential data assets.

The SAP Policy

At the recommendation of the Interagency Council on Statistical Policy (ICSP), the SAP Policy establishes the SAP to be implemented by the Federal statistical agencies and units and incorporates directives from the Evidence Act. The policy is intended to provide guidance as to the application and review processes using the SAP Portal, setting forth clear standards that enable Federal statistical agencies and units to implement a common application form and a uniform review process. The SAP Policy was submitted to the public for comment in January 2022 ([87 FR 2459](#)). The policy was finalized and published on December 8, 2022.²

The SAP Portal Process

Submitting an Application through the SAP Portal

The SAP Portal

²<https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-04.pdf>

The SAP Portal is an application interface connecting applicants seeking data with a catalog of data assets owned by the Federal statistical agencies and units and is hosted at <http://www.researchdatagov.org>. The SAP Portal is not a new data repository or warehouse; confidential data assets will continue to be stored in secure data access facilities owned and hosted by the Federal statistical agencies and units. The SAP Portal will provide a streamlined application process across agencies, reducing redundancies in the application process. This single SAP Portal will improve the process for applicants, tracking and communicating the application process throughout its lifecycle. This reduces redundancies and burden on applicants who request access to data from multiple agencies. The SAP Portal will automate key tasks to save resources and time and will bring agencies into compliance with the Evidence Act statutory requirements.

Data Discovery

Individuals begin the process of accessing restricted use data by discovering confidential data assets through the SAP metadata catalog maintained by Federal statistical agencies at www.researchdatagov.org. Potential applicants can search by agency, topic, or keyword to identify data of interest or relevance. Once they have identified data of interest, applicants can view metadata outlining the title, description or abstract, scope and coverage, and detailed methodology related to a specific data asset to determine its relevance to their research.

While Federal statistical agencies and units shall endeavor to include metadata in the SAP catalog on all confidential data assets for which they accept applications, it may not be feasible to include metadata for some data assets (e.g., potential special tabulations of administrative data). A statistical agency or unit may still accept an application through the SAP Portal even if the requested data asset or special tabulation is not listed in the SAP metadata catalog.

SAP Application Process

Individuals who have identified and wish to access confidential data assets are able to apply for access through the SAP Portal, which was released to the public in late 2022 (www.researchdatagov.org). Applicants must create an account and follow all steps to complete the application. Applicants begin by entering their personal, contact, and institutional information, as well as the personal, contact, and institutional information of all individuals on their research team.

Applicants proceed to provide summary information about their proposed project, to include project title, duration, funding, timeline, and other details including the data asset(s) they are requesting and any proposed linkages to data not listed in the SAP data catalog, including non-Federal data sources. Applicants then proceed to enter detailed information regarding their proposed project, including a project abstract, research question(s), literature review, project scope, research methodology, project products, and anticipated output. Applicants must demonstrate a need for confidential data, outlining why their research question cannot be answered using publicly available information.

Submission for Review

Upon submission of their application, applicants will receive a notification that their application has been received and is under review by the data-owning agency or agencies (in the event where

data assets are requested from multiple agencies). At this point, applicants will also be notified that application approval does not alone grant access to confidential data, and that, if approved, applicants must comply with the data-owning agency's security requirements outside of the SAP Portal, which may include a background check.

In accordance with the Evidence Act and the direction of the ICSP, Federal agencies will approve or reject an application within a prompt timeframe. In some cases, Federal agencies may determine that additional clarity, information, or modification is needed and request the applicant to "revise and resubmit" their application.

Data discovery, the SAP application process, and the submission for review are planned to take place within the web-based SAP Portal. As noted above, the notice announcing plans to collect information through the SAP Portal was published separately in the Federal Register ([87 FR 53793-53795](https://www.federalregister.gov/documents/2022/09/01/2022-08795))³ on September 1, 2022. (See footnote 1 for more information about the SAP Policy.)

Access to Restricted Use Data

In the event of a positive determination, the applicant will be notified that their proposal has been accepted. The final determination (positive or adverse) concludes the SAP Portal process. In the instance of a positive determination, the data-owning agency (or agencies) will contact the applicant to provide instructions on the agency's security requirements that must be completed to gain access to the confidential data. The completion and submission of the agency's security requirements will take place outside of the SAP Portal.

Collection of Information for Data Security Requirements

In the instance of a positive determination for an application requesting access to NAHMS-owned confidential data asset, APHIS–NAHMS will contact the applicant(s) to initiate the process of collecting information to fulfill its data security requirements. This process allows APHIS–NAHMS to place the applicant(s) in a trusted access category and includes the collection of the following information from applicant(s):

- Training requirements:
 - For datasets owned by APHIS–NAHMS, completion of a *NAHMS Data Access Security Briefing*, which will include training on data protections and the laws, including the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2018 (Title III of Public Law 115–435, codified in 44 U.S.C. Ch. 35), which provide the data protections afforded NAHMS study data, will be required prior to accessing the restricted use data. CIPSEA stands for.
 - For datasets owned by USDA's National Agricultural Statistics Service (NASS) and NAHMS, NASS personnel will provide a *NASS Data Access Security Briefing* to all applicants who were approved access to restricted use data. The briefing will include information on CIPSEA and other applicable Federal laws that protect the restricted use data as well as preparing and submitting disclosure reviews.

³https://www.regulations.gov/document/NSF_FRDOC_0001-2997

- For datasets owned by NASS and NAHMS, applicants will be provided with the *USDA NASS Data Lab Handbook* that explains the policies and procedures associated with accessing unpublished NASS data in a NASS Data Lab (including data enclaves). Each researcher approved to access unpublished NASS data is required to sign the *NASS ADM-044: User Attestation* to acknowledge they were provided with the *USDA NASS Data Lab Handbook* and agree to abide by its provisions.
- Appointment of agency:
 - Applicants will complete and sign the *NAHMS Agent Agreement* form. This form appoints the approved applicant as an agent of NAHMS, specifies the data to which the agreement applies and the conditions by which the agent must adhere to protect the confidentiality of the data, provides citations and excerpts from applicable laws under which data are protected, and requires a signature by the applicant.
 - For datasets owned by NASS and NAHMS, the applicants will complete and sign the *NASS ADM-043: Certification and Restrictions on Use of Unpublished Data*. This form is required to be signed by researchers who have been approved to access unpublished NASS data. The form contains excerpts of the various laws that apply to the unpublished data being provided to the applicant. The form explains the restrictions associated with the unpublished data and includes a place for the applicant to sign the form, thereby acknowledging the restrictions and agreeing to abide by them.
- Physical or virtual Data Lab security requirement:
 - The *NAHMS Data Lab Security Briefing*, which outlines the processes and procedures regarding gaining access to, working within, and requesting output from the USDA information technology system in the physical NAHMS Data Lab in Fort Collins, CO.
 - If virtual enclave access is requested, the applicant will be required to complete a site inspection with NAHMS personnel (using the *NAHMS Site Inspection Checklist*) or NASS personnel (using the *NASS ADM-045: Site Inspection Checklist*), which gathers information about the physical environment and the computer that the applicant will use to gain access to the virtual enclave.

A flow chart outlining the general SAP Portal application process can be found in Figure 1 (below). A flow chart detailing the steps needed to complete the data security requirements can be found in Figure 2 (below).

Note that the training requirements and security agreements listed above are for researchers requesting access to NAHMS-owned data or NASS and NAHMS co-owned data. The burden and cost estimates associated with this information collection request (ICR) account for both. NAHMS and NASS have agreed to report the burden and cost estimates for the NASS activities above under this ICR, and the NASS activities will be merged into the NASS ICR ([0535-0274](#)) upon its next renewal.

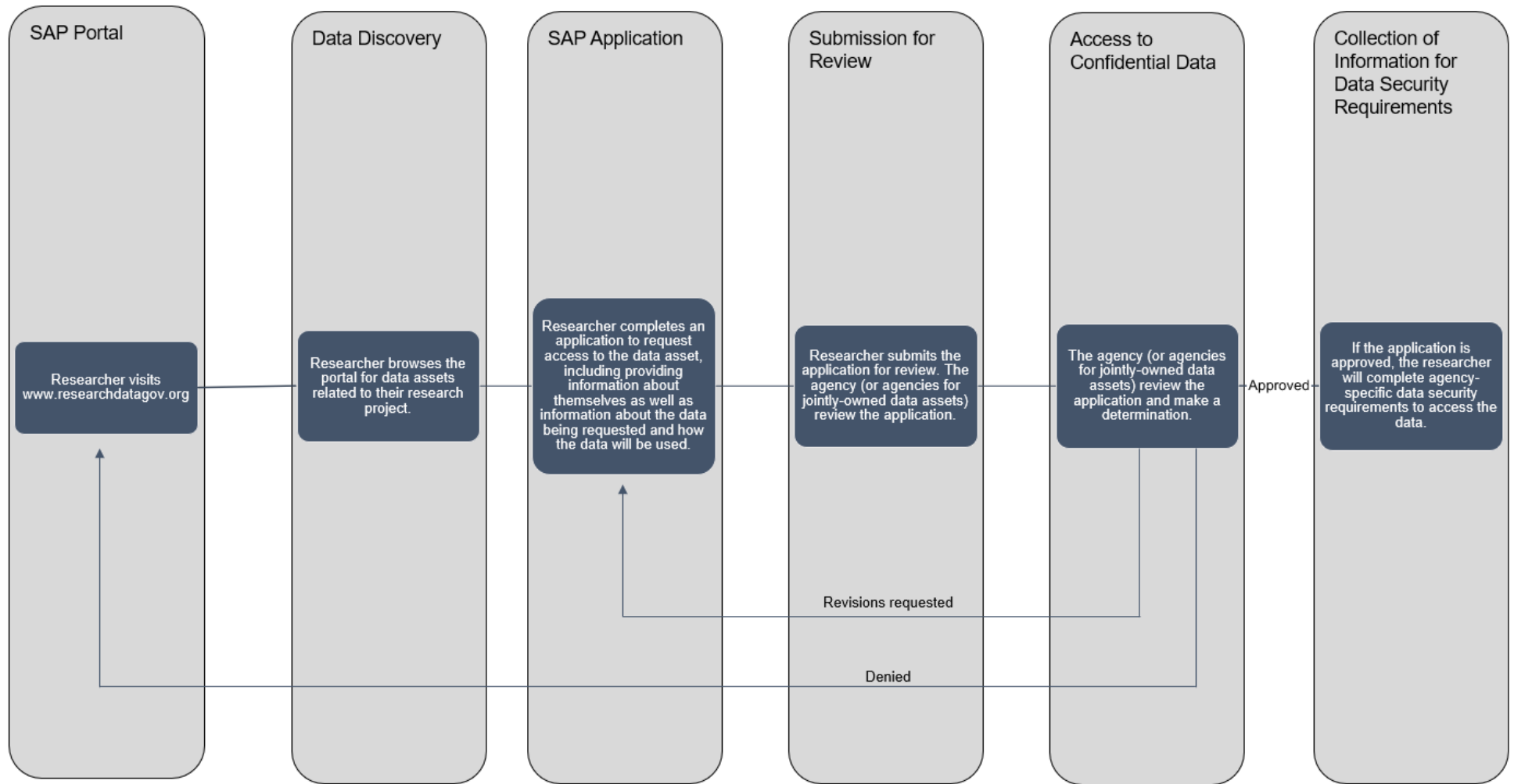


Figure 1: SAP requirement for portal application submission.

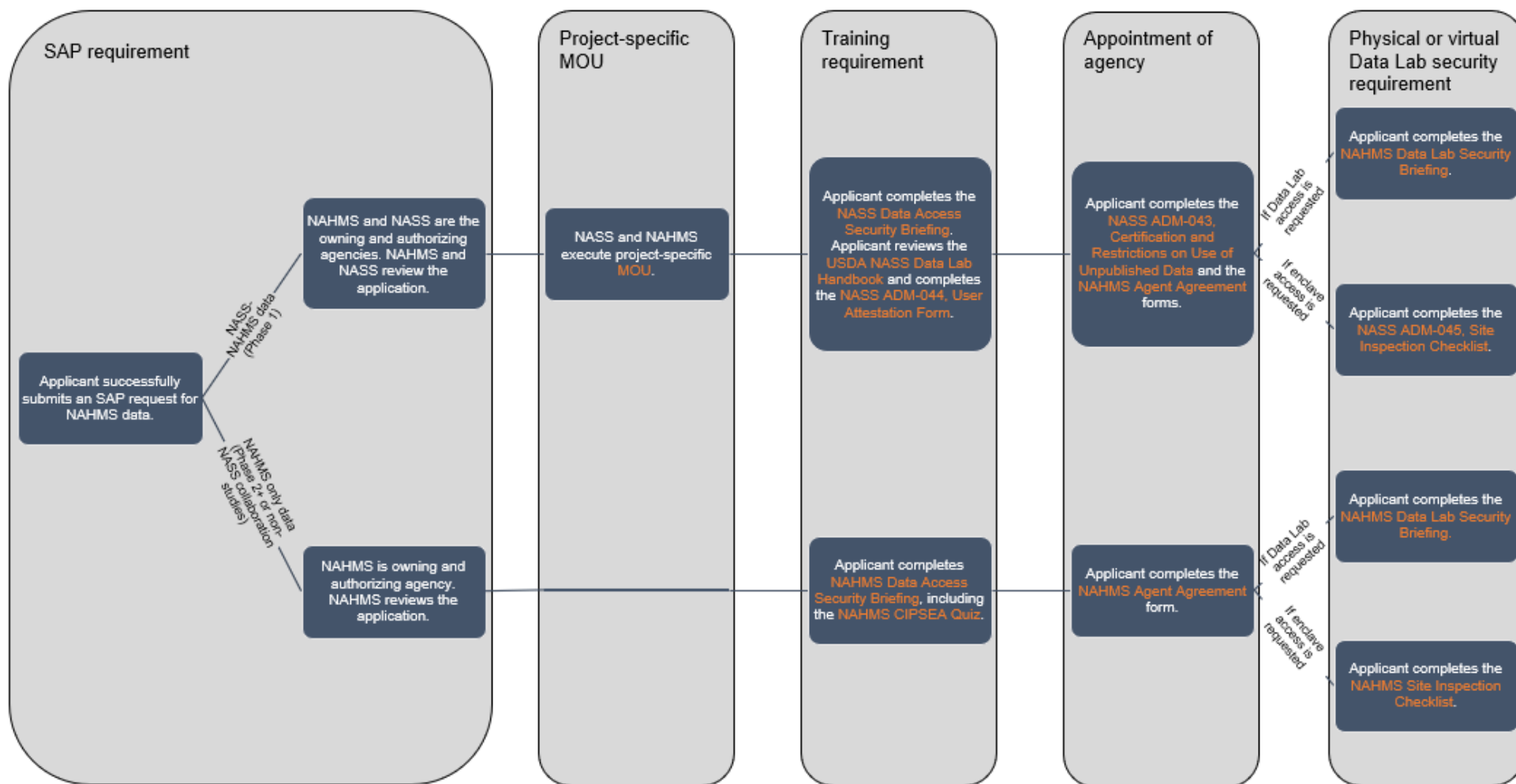


Figure 2: Collection of data security requirements for both NASS-NAHMS datasets and for NAHMS-only datasets.

Authorization

This collection is authorized by the Confidential Information Protection and Statistical Efficiency Act of 2018, Title III of Pub. L. No. 115-435, codified in 44 U.S.C. Ch. 35.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

The Paperwork Reduction Act (PRA) seeks to maximize the usefulness of information created, collected, maintained, used, shared, and disseminated by or for the Federal government while also ensuring the greatest possible public benefit from such information. The PRA, moreover, mandates that the disposition of information by or for the Federal government is consistent with laws related to privacy and confidentiality. APHIS–NAHMS’ data security agreements ensure that APHIS–NAHMS is compliant with PRA requirements.

Data collected, accessed, or acquired by statistical agencies and units is vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. Access to confidential data on businesses, households, and individuals from Federal statistical agencies and units enables agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals to contribute evidence-based information to research and policy questions on economic, social, and environmental issues of national, regional, and local importance. This evidence can benefit the stakeholders in the programs, the broader public, as well as policymakers and program managers at the Federal, State, local, and Tribal levels.

Many applicants will be academic research faculty or students at U.S. universities or other types of research institutions. Other applicants are likely to include analysts at nonprofit organizations and research groups in U.S. Government organizations (Federal, State, local, and Tribal). Scientific research typically results in papers presented at scientific conferences and published in peer-reviewed academic journals, working paper series, monographs, and technical reports. The scientific community at large benefits from the additions to knowledge resulting from research with statistical agencies and units’ data. Results inform both scientific theory and public policy and can assist agencies in carrying out their missions.

Approved applicants using confidential data can provide insights on how statistical agencies and units may improve the quality of the data collected or acquired; identify shortcomings of current data collection programs and data processing methods; document new data needs; and develop methods to address survey nonresponse or improve statistical weights.

Data Collection Activities and Forms

The activities and forms applicable to this information collection are described below. Because APHIS–NAHMS maintains data assets co-owned by NASS, there are data security requirements that need to be met for both agencies when access is requested for datasets owned by both agencies. In order to keep duplication of data security requirements to a minimum, some of the activities described below are carried out by NASS personnel, and some of the forms are NASS forms, which are included under OMB control number 0535-0274. The activities carried out by NASS personnel and the NASS forms are prefixed with “NASS” below, while the activities carried out by APHIS–NAHMS and the APHIS–NAHMS forms are prefixed with “NAHMS” below.

NAHMS Activities

NAHMS Data Access Security Briefing; 44 U.S.C. 35; State, Local, Tribal Government

For datasets owned by APHIS–NAHMS, APHIS–NAHMS personnel will administer training to the applicant prior to their completion of the necessary forms below. The briefing includes information on the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA), Title III of Pub. L. No. 115-435, codified in 44 U.S.C. Ch. 35 and other applicable Federal laws that protect the restricted use data, along with basic information on proper handling of protected data. The security briefing is not included within this package submission for security purposes but can be produced upon request.

NAHMS Agent Agreement; 44 U.S.C. 35; State, Local, Tribal Government

For datasets owned by APHIS–NAHMS, APHIS–NAHMS personnel will provide this document to the applicant to review and sign. The form designates agency status to the applicant for access of protected APHIS–NAHMS data, as described in Section 3572 of U.S.C. 44. The form contains excerpts of the various laws that apply to the unpublished data being provided to the applicant. The form explains the restrictions associated with the unpublished data and includes a place for the applicant to sign the form, thereby acknowledging the restrictions and agreeing to abide by them.

NAHMS Site Inspection Checklist; 44 U.S.C. 35; State, Local, Tribal Government

If virtual enclave access is requested, and for datasets owned by APHIS–NAHMS, APHIS–NAHMS personnel will complete this form during a virtual or physical inspection of the site from which the applicant will access the virtual enclave. The form gathers information about the physical environment and the computer that the applicant will use to gain access to the virtual enclave.

NAHMS Data Lab Security Briefing; 44 U.S.C. 35; State, Local, Tribal Government

If physical data lab access is requested, APHIS–NAHMS personnel will administer this training to the applicant. This training outlines the processes and procedures regarding gaining access to, working within, and requesting output from USDA information technology systems in the physical NAHMS Data Lab in Fort Collins, CO. The security briefing is not included within this package submission for security purposes but can be produced upon request.

NASS Activities

NASS Data Access Security Briefing; 44 U.S.C. 35; State, Local, Tribal Government

For datasets owned by NASS and APHIS–NAHMS, NASS personnel will provide training to the applicant prior to their completion of the necessary forms below. The briefing includes information on the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA), Title III of Pub. L. No. 115-435, codified in 44 U.S.C. Ch. 35 and other applicable Federal laws that protect the restricted use data as well as preparing and submitting disclosure reviews. The security briefing is not included within this package submission for security purposes but can be produced upon request.

USDA NASS Data Lab Handbook; 44 U.S.C. 35; State, Local, Tribal Government

For datasets owned by NASS and APHIS–NAHMS, NASS personnel will provide this document to the applicant to review prior to their completion of the necessary forms below. This document contains information on the policies and procedures associated with accessing unpublished NASS data in a NASS Data Lab (including data enclaves). The security briefing is not included within this package submission for security purposes but can be produced upon request.

NASS ADM-044, User Attestation; 44 U.S.C. 35; State, Local, Tribal Government

For datasets owned by NASS and APHIS–NAHMS, NASS personnel will provide this form to approved researchers to acknowledge they were provided with the **USDA NASS Data Lab Handbook** and agree to abide by its provisions.

NASS ADM-043, Certification and Restrictions on Use of Unpublished Data; 44 U.S.C. 35; State, Local, Tribal Government

For datasets owned by NASS and APHIS–NAHMS, NASS personnel will provide this form to the applicant to review and sign. The form designates agency status to the applicant for access to protected NASS data, as described in Section 3572 of U.S.C. 44. The form contains excerpts of the various laws that apply to the unpublished data being provided to the applicant. The form explains the restrictions associated with the unpublished data and includes a place for the applicant to sign the form, thereby acknowledging the restrictions and agreeing to abide by them.

NASS ADM-045, Site Inspection Checklist; 44 U.S.C. 35; State, Local, Tribal Government

If virtual enclave access is requested, and for datasets owned by NASS and APHIS–NAHMS, NASS personnel will complete this form during a virtual or physical inspection of the site from which the applicant will access the virtual enclave. The form gathers information about the physical environment and the computer that the applicant will use to gain access to the virtual enclave.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g. permitting electronic submission of responses, and

the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

APHIS makes every effort to comply with the E-Government Act, 2002 (E-Gov) and to provide for alternative submission of information collections. APHIS–NAHMS will contact individuals requesting access to confidential data via email. This collection does not currently deploy any web-based systems and there are no future plans to make a web-based system for applicants to meet all of the data security requirements. Forms will be in fillable PDF format, and trainings will be provided either in a training session held over an electronic communication application or will be provided as electronic files to the applicant.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purpose(s) described in item 2 above.

APHIS–NAHMS is required by law to maintain careful controls on confidentiality and limit disclosure risk. Its security forms are required for each approved research project to ensure minimal disclosure risk of APHIS–NAHMS’ confidential data. APHIS–NAHMS has reviewed its security requirements to eliminate duplication.

There is no similar data collection available. Every effort has been made to avoid duplication. The agency has reviewed USDA reporting requirements, state administrative agency reporting requirements, and special studies by other government and private agencies. APHIS solely monitors APHIS–NAHMS to ensure integrity. The information required for data collection is not currently reported to any other agency on a regular basis in a standardized form.

5. If the collection of information impacts small businesses or other small entities, describe the methods used to minimize burden.

APHIS–NAHMS projects that the majority of applicants will not be members of small entities but assumes that 2 of the 10 (20 percent) expected applicants, over three years, will be members of small entities. Small businesses or their representatives may choose to participate in this voluntary collection of information. The burden of this collection does not represent a significant barrier to participation from small businesses and is not large enough to pose significant costs to respondents, including small businesses.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

This is an ongoing information collection request. Responses are voluntary; however, without them, applicants will not gain access to the SAP portal.

APHIS–NAHMS requires and collects information for its security forms for all individuals who will access data and output that has not been cleared for disclosure review. Less frequent collection would compromise APHIS–NAHMS’ ability to secure its confidential data.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5

- **requiring respondents to report information to the agency more often than quarterly;**
- **requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;**
- **requiring respondents to submit more than an original and two copies of any document;**
- **requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than 3 years;**
- **in connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study;**
- **requiring the use of a statistical data classification that has not been reviewed and approved by OMB;**
- **that includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or**
- **requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.**

No special circumstances exist that would require this collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5.

8. Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting form, and on the data elements to be recorded, disclosed, or reported. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency’s notice, soliciting comments on the information collection prior to submission to OMB.

The language in the current submission was developed in collaboration with USDA NASS and other Federal statistical agencies and units in the SAP Technical Working Group. The steps outlined in Question 1 and in Figure 2 were developed in collaboration with NASS to ensure that the data security requirements for both agencies were met for datasets under both agencies.

On August 19, 2024, APHIS–NAHMS published a notice in the Federal Register (89 FR 67058) inviting the public and other Federal agencies to comment on plans to submit this request. APHIS–NAHMS received one comment requesting further information on the Evidence-Based Policymaking Act of 2018 (44 U.S.C. 3583) and the SAP process as they relate to keeping data on cattle secure. APHIS-NAHMS provided the information. APHIS-NAHMS received two additional comments via Regulations.gov referencing electronic identification tags for cattle and the Federal Animal Disease Traceability Rule. Neither of these comments are relevant to nor do they impact this information collection request.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No payments or gifts are given to holders of user accounts in the system.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

All personal identifiers are protected under the Privacy Act of 1974 and APHIS–NAHMS’ confidentiality privacy and practices. This information collection is authorized under the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA), Title III of Pub. L. No. 115-435, codified in 44 U.S.C. Ch. 35. The data confidentiality protections provided under that law will be used to protect the confidentiality of the data collected as a part of this information collection.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

There are no questions of a sensitive nature used in this collection activity.

12. Provide estimates of the hour burden of the collection of information.

- **Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in item 13 of OMB form 83-I.**

See APHIS 71. The agency estimates there will be 10 respondents and 26 hours of burden for this study annually. Over a three-year period, it is expected that there will be 30 respondents and 78 hours of burden.

The amount of time to complete the agreements and other paperwork that comprise APHIS–NAHMS’ security requirements will vary based on the confidential data assets requested. In order to obtain access to APHIS–NAHMS confidential data assets, it is estimated that the average time to complete and submit APHIS–NAHMS’ data security agreements and other paperwork is 156 minutes. This estimate does not include the time needed to complete and submit an application within the SAP Portal. All efforts related to SAP Portal applications are cited in ICR 3145-0271 and take place prior to and separate from APHIS–NAHMS’ effort to collect information related to data security requirements.

The expected number of applications in the SAP Portal that receive a positive determination from APHIS–NAHMS in a given year may vary. Overall, per year, APHIS–NAHMS estimates it will collect data security information for 10 application submissions that received a positive determination within the SAP Portal. Furthermore, the burden estimates below assume that, of the 10 applicants, we expect to have 5 requests for data co-owned by APHIS–NAHMS and NASS, of which all 5 will access the data using the virtual data enclave; and 5 requests for APHIS–NAHMS data, of which 3 will access the data through the virtual data enclave and 2 through the physical data lab. APHIS–NAHMS estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 78 hours and, as a result, an average annual burden of 26 hours.

- Type of submission: Data access and security training, appointment of agency paperwork
 - Average submission time: 156 minutes
 - Annual number of security form submissions: 10 applications
 - Total burden hours over the three-year OMB clearance: 3 years x 156 minutes x 10 applications = 4,680 minutes / 60 minutes = 78 hours
 - Annual burden hours over the three-year OMB clearance: 78 hours / 3 years = 26 hours
-
- **Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using the correct wage rate categories.**

The total annualized cost to applications requesting access to APHIS–NAHMS data for the 26 total burden hours is estimated to be \$963, or the total three-year cost to applicants of \$2,889.

This estimate is based on an estimated median annual salary of \$77,000 per applicant, where estimated annual salary information was sourced from the annual median salary estimates for employed college graduates using data from the 2021 National Survey of College Graduates

(<https://nces.nsf.gov/surveys/national-survey-college-graduates/2021>). Assuming a 40-

hour workweek and a 52-week salary, this annual salary translates to an hourly salary of \$37.02.

13. Provide estimates of the total annual cost burden to respondents or recordkeepers resulting from the collection of information. (Do not include the cost of any hour burden shown in items 12 and 14). The cost estimates should be split into two components: (a) a total capital and start-up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of services component.

There are no capital/start-up or ongoing operation/maintenance costs associated with this information collection.

14. Provide estimates of annualized cost to the Federal government. Provide a description of the method used to estimate cost and any other expense that would not have been incurred without this collection of information.

See APHIS 79. The estimated cost to the Federal Government is \$1,323.

15. Explain the reasons for any program changes or adjustments reported in items 13 or 14 of the OMB Form 83-I.

This is a new information collection request and consists of an estimated 10 respondents, 52 annual responses, and 26 hours of burden. APHIS-NAHMS estimates there will be 6 responses per respondent with each response being approximately 30 minutes.

16. For collections of information whose results will be published, outline plans for tabulation and publication.

The information collected will not be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

The OMB approval expiration date will be displayed on the instruments.

18. Explain each exception to the certification statement identified in the "Certification for Paperwork Reduction Act."

APHIS is able to certify compliance with all provisions in the Paperwork Reduction Act.