Privacy Impact Assessment

National Bio Agro-Defense Facility (NBAF) AZURE Information Laboratory System (NAILS)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: April 7, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Document Information

Owner Details	
Name	Kenneth Burton
Contact Number	785-477-3200
E-mail Address	Kenneth.R.Burton@usda.gov

Document Revision and History

Revision	Date	Author	Comments
1.0	1APR20	Eric Fong	Initial Draft for NAILS
1.1	3APR20	Shah Mohammed	Secondary Review and Correction
1.2	3APR20	Eric Fong	Submit for Internal Review
1.3	6APR20	Eric Fong	Correction made, resubmit for review
1.4	7APR20	Eric Fong	Return from internal review, submit for privacy review
1.4	14APR20	Eric Fong Shah Mohammend	Privacy review complete, routing for signatures

Distribution List

Name	Title	Agency/Office	Contact Information
Kenneth Burton	System Owner	NBAF	Kenneth.R.Burton@usda.gov

Privacy Impact Assessment for the

NBAF Azure Information and Laboratory System
7 April 2020

Contact Point

Eric Fong
Information Systems Security Manager
APHIS/NBAF
(785) 477-3496

Reviewing Official

Tonya Woods
Privacy Act Director
United States Department of Agriculture
(301) 851-4072

Kenneth Burton
NBAF Coordinator
United States Department of Agriculture
(785) 712-3011

Overview

The primary mission of the NBAF is the protection of animal health for the United States livestock industry. Capabilities for the NBAF include laboratories designed, constructed, and equipped for Biosafety Level (BSL) 2, 3 and 4. NBAF strengthen U.S. capability for training veterinarians to quickly identify foreign animal and zoonotic diseases in the field, reducing the impact of a potential outbreak.

The purpose of the USDA National Bio and Agro-defense Faculty (NBAF) Azure Information and Laboratory System (NAILS) to support and authorize applications in the Veterinary Services (VS) subscription hosted in Marketing and Regulatory Programs (MRP) Animal and Plant Health Inspection Service (APHIS) Azure Cloud in use by the NBAF located at Manhattan, Kansas. NBAF is charged with basic and applied research, diagnostics, training, and the development of countermeasures for foreign animal and zoonotic diseases. This PIA was conducted because the NAILS has the potential to store personally identifiable information within the file servers. Currently the NAILS Risk Management Framework (RMF) activities are ongoing with a planned completion date of July, 2020.

The function of the system is to deliver the following services to NBAF:

Environmental, Health, Safety and Quality (EHSQ)
Biological Information Management System (BioIMS)
Electronic Laboratory Notebook (ELN)
Animal Management System (AMS)

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 (NBAF) Azure Information and Laboratory System (NAILS) stores data used and processed by laboratory and administrative information on procedures, policies, instructions, references, manuals, forms, audits, calibration results, and reports.
The Marketing and Regulatory Programs (MRP) Animal and Plant Health Inspection Service (APHIS) Azure Cloud maintains the data and is responsible

for the security of the stored data. The applications in NAILS may contain PII information on individuals to include:

☒ Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias).

☒ Date and/or place of birth.

☒ Address Information (street or email address).

☒ Personal identification number (e.g. social security number, tax identification number, passport number, driver's license number or a unique identification number, etc)

☐ Financial data (credit card numbers, bank account numbers, etc.).

☒ Animal Health data (including height, weight, blood pressure, etc.).

☐ Biometric data (fingerprints, iris scans, voice signature, facial geometry, DNA, etc.).

☐ Criminal history.

☐ Employment history.

☒ Miscellaneous identification numbers (agency assigned number, case number, accounts, permits, etc.).

☒ Photographic image/identifying characteristics.

☒ Handwriting or an image of the signature.

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

The source of the information on containing data come for the USDA users that inputs in NAILS applications and the Active Directory (AD). The stored information is for the USDA Animal and Plant Health Inspection Service (APHIS) employees/contractors for support of the NBAF mission.

All users will require Domain Account Request Form to access NAILS. This information is the minimum required to approve the applicable account request form. This ensures that while the user is using IT resources under one single Enterprise Active Directory that their actions can be audited. Users must complete Information Awareness (IA) per the ***Acceptable Use Policy*** (AUP) and ***Rules of Behavior*** (ROB) to gain access to NBAF Domain. ***Non-Disclosure Agreement*** (NDA) for NBAF contractors is additional requirement for contractors.

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

The information is maintained in NAILS to maintain compliance with the Laboratories' accreditation, Animal Management accreditation, and Safety, Health, Environmental accreditation. Collecting the information listed in Sections 1.1 and 1.2 of this document helps automate, streamline, and manage the following under a single web based platform: animal health data, safety and environment management related data, regulatory compliance, laboratory management data, standard operating procedures (SOPs), work instructions (WI), references, manuals, forms, laboratory audits (internal audits of laboratory activities, administrative procedures, calibration), and metric reports.

1.4 How is the information collected?

The information is collected by applications, servers maintained by Marketing and Regulatory Programs (MRP) Animal and Plant Health Inspection Service (APHIS) Azure Cloud Veterinary Service (VS) Subscription. Employee information is collected from the supervisor, USDA active directory.

Domain and Application Accounts - The information is submitted on the Domain Account Request Form and User Management System (UMS) approved by their supervisor. All users are requested to have a Domain Account Request access NAILS, see 1.2.

1.5 How will the information be checked for accuracy?

Employee information is validated by the individual's supervisor through the use of an Animal and Plant Health Inspection Service (APHIS) 513 form, digitized in the User Management System (UMS).

Domain accounts in Sections 1.1 and 1.2 is checked for accuracy via review (such as background check, suitability review), quality and document managers, and the employee's supervisor. After the employee's supervisor approves the document, the document is then sent to the appropriate Program quality manager for final review/authorization.

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

Specific legal authorities for applications in NAILS include:

Homeland Security Presidential Directive 9 (HSPD-9).
Virus-Serum –Toxin Act (21 USC §151-159 et.seq.)
9 CFR 53 (Foot-And-Mouth Disease, Pleuropneumonia, Rinderpest, and Certain other communicable Diseases of Livestock or Poultry)
9 CFR 56 (Control of H5/H7 Low Pathogenic Avian Influenza)
9 CFR 82 (Exotic Newcastle Diseases and Chlamydiosis)
9 CFR 94 (Rinderpest, Foot-and-Mouth Disease, Exotic Newcastle Disease, African Swine Fever, Classical Swine Fever, Swine Vesicular Disease, and Bovine Spongiform Encephalopathy: prohibited and restricted importations)

9 CFR 121 (Possession, Use, And Transfer Of Select Agents And Toxins)
Animal Health Protection Act (7 USC Chapter 109)
Animal Welfare Act (7 USC 54)
Homeland Security Presidential Directives (HSPD) 5 (Management of Domestic Incidents)
HSPD 7 (Critical Infrastructure Identification, Prioritization, and Protection)
HSPD 8 (National Preparedness)
HSPD 9 (Defense of United States Agriculture and Food)
HSPD 12 (Policies for a common Identification Standard for Federal Employees and Contractors)
The Organic Act of 1862 (7 U.S.C. 2201 note)

Agricultural Research Act of 1935 (7 U.S.C. 427)

Research and Marketing Act of 1946 (Pub. L. 79-733), as amended (7 U.S.C. 427, 1621 note)

Food and Agriculture Act of 1977 (Pub. L. 95- 113), as amended (7 U.S.C. 1281 note)

Food Security Act of 1985 (Pub. L. 99-198) (7 U.S.C. 3101 note)

Food, Agriculture, Conservation, and Trade Act of 1990 (Pub. L. 101-624) (7 U.S.C. 1421 note)

Federal Agriculture Improvement and Reform Act of 1996 (Pub. L. 104-127)

Agricultural Research, Extension, and Education Reform Act of 1998 (Pub. L. 105-185)

Farm Security and Rural Investment Act of 2002 (Pub.L. 107-171).

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

To minimize privacy risks, all user access is granted in the start after the completion of Information Awareness (IA) per the Acceptable Use Policy (AUP) and Rules of Behavior (ROB) and re-verify annually. Access is limited to USDA employees only, Need to Know (NtK) basis.

Employee information is validated by the individual’s supervisor through the use of an Animal and Plant Health Inspection Service (APHIS) 513 form, digitized in the User Management System (UMS).

Unauthorized access to this data is the privacy risk. This is mitigated by using capabilities common to USDA and the commercial products used. This includes:
- System access control by USDA domain credentials
- User based role access
- Separation of duties
- Limiting web access

- Audit logging
- Standard Operating Procedures (SOPs)

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.

National Bio Agro-Defense Facility (NBAF) Azure Information Laboratory System (NAILS) is categories as a moderate system. Information used in NAILS help to automate, streamline and manage the following under a single web-based platform:

- Environmental, Health, Safety and Quality (EHSQ) – Information is used by Animal and Plant Health Inspection Service (APHIS) to meet compliance with all **regulatory requirements and ISO accreditation.**
- Biological Information Management System (BioIMS) - Information is used by APHIS VS NBAF to manage **laboratory inventory data, workflow, and to meet all regulatory requirements and ISO accreditation**.
- Electronic Laboratory Notebook (ELN) – Information enable researchers to store and organize research laboratory and animal data.
- Animal Management System (AMS) – Information is used to maintain **animal inventory, animal health data, quality management, and to meet compliance with all regulatory requirements and ISO accreditation.**

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

Biological Information Management System (BioIMS) - Biological Information Management System Commercial off the Shelf (COTS) that contains automate and streamline processes to include:

- Study Management
- Reports
- Analytic Quality Control
- Storage Management
- Workflow
- Sample Tests and Results

Environmental, Health, Safety and Quality (EHSQ) COTS that contains automate and streamline processes to include:

- Safety Process
- Compliance Management
- Operational Efficiency
- ISO Accreditation
- Compliance Management
- Document Control

Animal Management System:

- Animal Ordering
- Inventory Management
- Order Control
- Compliance Management

Electronic Health Notebook

- Inventory Management
- Research Management
- Inventory Management

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

Applications may utilize publicly available ISO accreditation requirements to maintain ISO accreditation, A2LA (an accrediting body with additional requirements that is used for clarification/guidance of ISO requirements), equipment manuals and vendor websites (for instrumentation), and also scientific journal articles for scientific test validation.

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.

Technical:

- NAILS applications use Enterprise Active Directory (EAD) controls and security policies within MRP Animal and Plant Health Inspection Service (APHIS) Azure Cloud.
- The security of the information being passed on this two-way connection is protected using FIPS 140-2 approved encryption mechanisms.

- Employee information is validated by the individual's supervisor through the use of an APHIS 513 form, digitized in the User Management System (UMS).

Administrative:

- Users have formal training on how to properly manage PII.
- Users have formal training in how to use the system.
- All access to the system is limited to authorized personnel only with the "Need to Know".
- Access to the data in the system is controlled and documented by formal authorization.

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?

According to https://www.archives.gov/files/records-mgmt/grs/grs04-1.pdf, "Items are retained per the General Records Schedule 4.1: this is vital records program records - Destroy 3 years after project, activity, or transaction is completed or superseded, but longer retention is authorized. The data is retained as per specified for system backup and tape libraries. Data is backed up as a monthly full backup, with daily incremental backups, and then superseded by the next full backup. Data is retained for 3 years."

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

Each of the program offices that collect data will schedule the records as required. Data is backed up as a monthly full backup, with daily incremental backups, and then superseded by the next full backup. Data is retained for 3 years or based on SOPs and regulations.

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

The risk would be keeping data exceeding the time needed.

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?

This information may be used by components of USDA to include Agricultural Marketing Service (AMS), Animal and Plant Health Inspection Service (APHIS), Agricultural Research Service (ARS), Office of the General Counsel (OGC), Officer of Inspector General (OIG) and other USDA agencies. Information is also shared with USDA ARS employees co-located with NVSL at the Foreign Animal Disease Diagnostic Laboratory (FADDL) in Plum Island, NY.

4.2 How is the information transmitted or disclosed?

This is based on the programs use of the data and this would be documented in the appropriate PIA and/or SORN.

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.

Information is not shared outside of USDA.

All NAILS systems also have administrative as well as technical security controls to address access to and security of information.

All information sharing with internal systems is done over the internal APHIS network.

Access to the data in the NAILS systems is controlled and documented by formal authorization.

All access to the system is limited by account identification and eAuthentication. The eAuthentication makes uses of Personal Identification Verification (PIV) cards using associated certificates.

Users have formal training in how to use the system

A warning banner must be acknowledged at login

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?

Information is not shared outside of USDA.

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.

Information is not shared outside of USDA.

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

Information is not shared outside of USDA.

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

Information is not shared outside of USDA. The NAILS is not publicly accessible. The procedures to allow individuals to gain access to their information is through the suitability process, contractors accessing the domain will require a Non-disclosure Agreement (NDA). In addition, all users are required to take the Information Security Awareness Training (ISAT) and sign the Rules of Behavior (ROB). To gain NAILS application access, it will require the individual’s supervisor approval. Mandatory application training is also mandatory to use the applications in NAILS.

Section 6.0 Notice

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

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

No.

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

Yes.

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

No.

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

No. The information is used for internal purposes only and not shared. All information is required to grant account access to ensure proper security and auditing. If the user does not consent to use of all requested information, the account request will likely be disapproved.
Only information that is cleared through the Freedom of Information Act is available for use.

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

There is no risk identified with individuals not being unaware of the collection of data. All data is provided by the user on the account request form.

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?

The APHIS Azure Cloud is not publicly accessible even though the applications may be publicly accessible. The procedures to allow individuals to gain access to their information is through the suitability process, contractors accessing the domain will require a Non-disclosure Agreement (NDA). In addition, all users are required to take the Information Security Awareness Training (ISAT) and sign the Rules of Behavior (ROB). To gain NAILS application access, it will require the individual’s supervisor approval.

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

The user can provide an updated account request to have the current information update. They will be required to provide supporting documentation justifying the change.

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

All USDA NBAF IT or admin employees are notified of the procedures to correct information by their human resource department.

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

Submit a Service Now ticket and assign to the NBAF Laboratory Endpoint System administrator.

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 risks are associated with the redress, all procedures are followed based on the requirements of privacy act.

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?

USDA requires ISAT (Information Security Awareness Training) and a Rules of Behavior (ROB) for which all users must consent to prior to being granted system credentials for access. The NAILS system inherits the USDA implementation of User Security Awareness training which is required annually and NAILS system has created Security Groups which will granulize the access a user has based on the idea of “Least Access Required” and also each system in NAILS utilities the User Management System (UMS) to assist in validating users periodically. A supervisor submits for an employee access to a system. Once an application is reviewed by the employee’s supervisor, the administrator of the application will be notified to review and add/remove user accounts.

8.2 Will Department contractors have access to the system?

Vetted contractors with USDA suitability clearance, Non-Disclosure Agreement (NDA), Information Awareness Training (IAT) training and agreement will have access to the system. Supervisors of the application will authorize the contractor access given the Need to Know (NtK).

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

All members are required to complete annual Information Technology (IT) Security Awareness Training and must sign APHIS Rules of Behavior form prior to receiving access to the information system. The standard USDA warning banner must also be acknowledged and accepted before logging in to the system.

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

The Certification and Accreditation is in the progress with the projected completion date of July 2020. This Privacy Impact Assessment will be used in support of the initial Authority to Operate (ATO) package that is being worked for this System.

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

Technical safeguards and auditing measures are in accordance with FIPS 199/200 Moderate Baseline Security Controls. Some of the technical safeguards are a security model that includes auditing, role-based views, field-level security, and division of security. This means any events, such as create, modify, soft deletion, and user login activity are audited at the field level. In addition, 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 for access to the data within Applications in NAILS is through role-based access and data restriction configurations. Furthermore, views and field-level access are role-based, preventing users from seeing, accessing, and/or making changes to individual fields or records they do not have access to. All NAILS users must be validated against APHIS Active Directory for authentication.

- All access to the data in the system is controlled by formal authorization using User Management System (UMS).
- All access to the system is limited by account identification and eAuthentication. The eAuthentication makes uses of PIV cards using associated certificates.
- USDA Active Directory (AD) provides authentication and identity services for this information system. All users must have active AD accounts for access.
- Warning banner must be acknowledged before logging in.
- All information sharing with internal systems is done over the internal APHIS network.
- Auditing is enabled both at the application and database level.

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?

This risk is mitigated through administrative user training and limiting use to Federal owned networks. Users are trained at least annually, and accounts are verified annually. Information is limited to APHIS, ARS systems. The integrity of the data is protected through AEI GSS to ensure all transaction are complete and all items shipped successfully. All data objects, transactions, and ship-to data are protected by the available USDA technology and services (Bitlocker, CheckPoint, GPO updates and Active Directory). Audit logs are available for all transactions.

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?

The National Bio and Agro-Defense Facility (NBAF) Azure Information and Laboratory System (NAILS) provide Commercial off the Shelf Software (COTS) to fulfill the mission of inspecting and protecting animal and plant materials, to maintain compliance and ISO accreditation, and security stores, processes research data across the Marketing and Regulatory Programs (MRP) Animal and Plant Health Inspection Service (APHIS) Azure Cloud.

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

Not Applicable.

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, The ISSPM and system owner have reviewed the OMB memorandums listed above.

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

No 3rd party web sites are used.

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

Not Applicable.

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

Not Applicable.

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?

Not Applicable.

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

Not Applicable.

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

Not Applicable.

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?

Not Applicable.

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)?

Not Applicable.

10.10 Does the system use web measurement and customization technology?

Not Applicable.

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?

Not Applicable.

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.

Not Applicable.

Responsible Officials

PRESTON GRIFFIN Digitally signed by PRESTON GRIFFIN
Date: 2020.05.05 10:47:08 -04'00'

Preston Griffin
MRP CISO or MRP ISSPM
Marketing and Regulatory Programs
United States Department of Agriculture

JANELLE JORDAN Digitally signed by JANELLE JORDAN
Date: 2020.04.24 06:08:39 -04'00'

Tonya G. Woods
APHIS Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture

KENNETH BURTON Digitally signed by KENNETH BURTON
Date: 2020.04.25 09:31:15 -05'00'

Kenneth Burton
System Owner
APHIS/NBAF
United States Department of Agriculture